Navy Marine Corps Intranet (NMCI) Legacy Systems Transition Guide (Risk Mitigation Phase)

Version 1.4

18 June 2004

Prepared by:
NMCI Program Management Office – Legacy Systems Division, PMW 164-4
Space and Naval Warfare Systems Command (SPAWAR)
Participants in the creation of this guide include:
Electronic Data Systems
Commander, Naval Network Warfare Command

Prepared for:

All NMCI Customers

TABLE OF CONTENTS

APPENDICES

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1.0 BACKGROUND

The Department of Navy's (DON) current information technology infrastructure is composed of multiple 'Stove-Pipe' systems and legacy networks, which are decentralized and managed at the system or program level. As a result, the Navy has limited or no interoperability, visibility, and communication capabilities across the enterprise. The Legacy Systems Transition Guide (LSTG) will outline the process to successfully transition legacy systems to the Navy Marine Corps Intranet (NMCI) environment facilitating a critical step in the DON's end-state goal of one intranet for CONUS shore installations.

NMCI (please refer to http://www.nmci-eds.com/nmci.htm) is a comprehensive, enterprise-wide initiative that will make the full range of network-based information services available to Sailors and Marines for day-to-day activities by applying the speed and might of world-class Internet technology to everything from administrative tasks to ammunition supply. NMCI will give the Navy and Marine Corps secure, universal access to integrated voice, video, and data communications. It will afford pier-side connectivity to Navy vessels in port. Also, it will link more than 360,000 desktops across the United States as well as sites in Puerto Rico, Iceland, and Cuba.

NMCI, along with IT-21 (Information Technology for the Twenty-first Century) and Base Level Information Infrastructure (BLII), will serve as the foundation of the DON's network centric approach. As a precursor to FORCEnet and Sea Power 21, NMCI will support the warfighter by integrating weapons, networks, and platforms and allowing the warfighter to focus on the mission rather than technology issues. Additionally, NMCI will help the Navy and Marine Corps meet these critical objectives:

- Enhanced network security.
- Interoperability across Commands and other Services.
- Knowledge sharing across the globe.
- Increased productivity.
- Improved systems reliability and quality of service.
- Reduced cost of voice, video, and data services.

To facilitate the aforementioned critical objectives, Navy and Marine Corps shore-based systems must reside in the NMCI environment. Therefore, legacy servers and supporting devices/ systems must transition from legacy environments to the NMCI environment. The NMCI DMZ, when available, which is logically outside NMCI environment is an option for connectivity to the NMCI Network

1.1 PURPOSE

The LSTG provides both an approach and the associated processes to successfully transition systems from legacy environments to the NMCI environment while maintaining or improving system performance and availability. The LSTG provides the Site Representative, Central Design Authority (CDA), and the Program Manager (PM) with the unique processes, tools/templates, and documentation guidelines to plan and execute the transition of their respective systems to the NMCI environment.

Due to the current decentralized approach, the DON has limited visibility into the total life cycle costs of systems and associated infrastructures. Consequently, the DON has limited buying power and reduced ability to take advantage of newer technologies across the enterprise. Figure 1-1 depicts the current NMCI architecture and security boundaries.

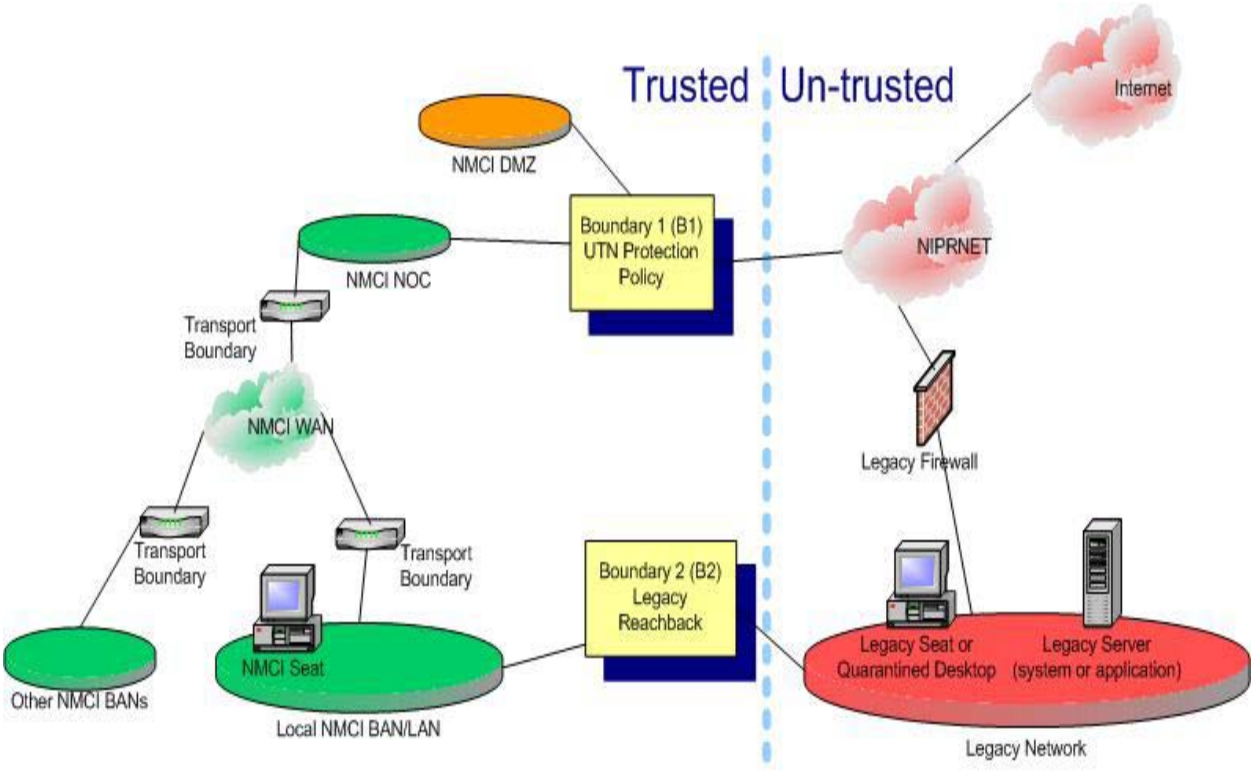


Figure 1-1 NMCI Architecture and Security Boundaries

As legacy systems are transitioned to NMCI and legacy networks are eliminated, the DON gains visibility into applications, systems, and infrastructure management at an enterprise level.

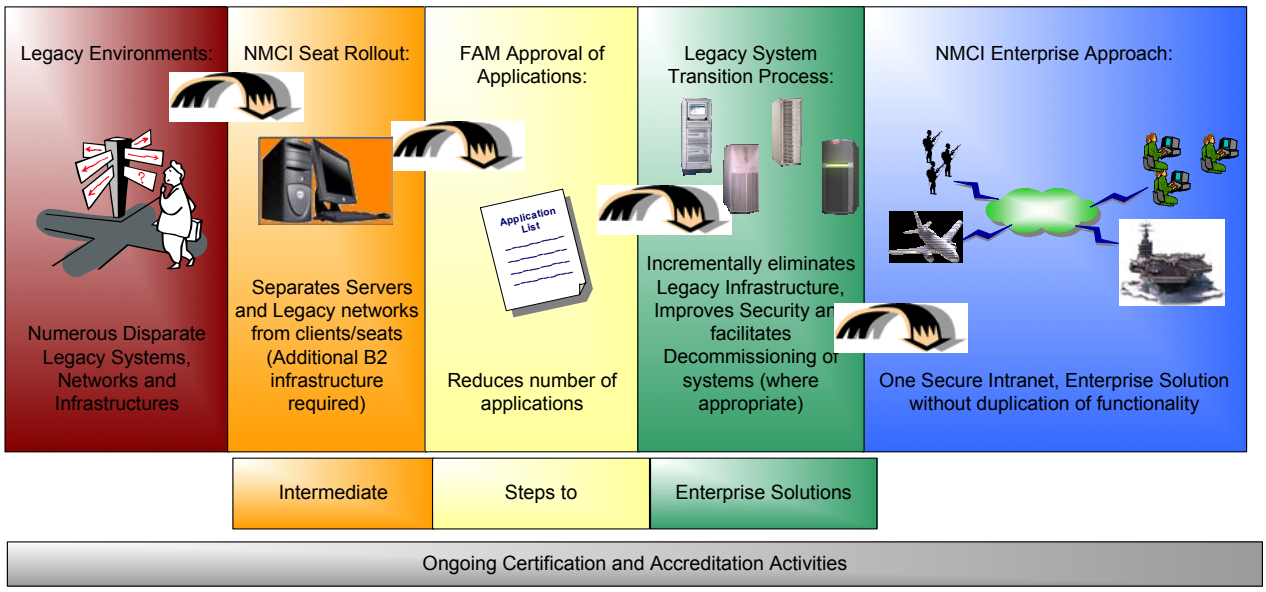


Figure 1-2 Path to NMCI Enterprise Solution

Additionally, the advantages of the newly centralized intranet are listed below:

- Improved performance.
  - Integrating end-to-end information services through a common computing and communications environment (enterprise solutions).
  - Eliminating interoperability problems.
  - Removing access, connectivity, and throughput as impediments to productivity and speed of command.
  - Centralizing configuration management and data center consolidation.

- Increased security.
  - Allowing the DON to quickly and securely share knowledge and information.
  - Implementing a centralized access control policy.
  - Reducing and consolidating data center facilities.
  - Implementing DON firewall policy.

- Reduced cost of operations (video, data, and voice services).
  - Eliminating legacy networks.
  - Standardizing and Consolidating Help Desks to form an Enterprise Help Desk.
  - Centralizing procurement to help manage the life cycle of equipment, licenses, maintenance agreements, and facilities.

- Reduced Quarantined seats.

A timely reduction of quarantined desktops and dual desktops is an advantage to the Site Representative, CDA and the PM to be in compliance with NMCI message 231700ZDEC02_OPNAV N6N7 which provides that the "maximum duration NMCI quarantined applications will be allowed to exist will be 6 months."

1.2 SCOPE

The scope of the LSTG is limited to the processes, procedures, and guidelines associated with successfully transitioning systems from the legacy DON environments to the NMCI environment. The Functional Area Manager (FAM)-approved systems intended for transition to the NMCI environment are included in the scope of the LSTG. Readers are encouraged to reference the DON Application & Database Management System (DADMS) located at https://www.dadms.navy.mil/DADMSProd/Register/menuRegister.cfm for the latest list of approved applications.

The LSTG only applies to "production or production ready" systems. Systems currently in development or testing, and Research and Development (R&D) Systems, are not in the scope for systems transitioning to NMCI.

Systems still in development and not yet providing user services at the time of cutover are considered emergent systems and are beyond the scope of the Legacy System Transition effort. Please refer to the Navy Enterprise Application Development Guide (NEADG) located at https://ucso2.hq.navy.mil/n09w/webbas01.nsf/(vwWebPage)/WebBase.htm?OpenDocument&Set=1 and the NMCI Release Development and Deployment Guide (NRDDG) for additional emergent system deployment information. For additional guidance, please refer to the Navy Enterprise and NMCI Process Guides in Figure 1-2 and subsequent guide descriptions.

Legacy Servers and Systems. Legacy applications and systems include existing customer software and hardware currently in use at a site by people performing the mission or business of the DON that are not included in the NMCI standard services or the Contract Line Item Number (CLIN) catalog. Legacy Systems may be individual servers housing one or more applications or systems consisting of multiple servers, console/workstations, supporting devices/systems, and possibly network devices. The current Legacy Systems may run any of several possible operating systems (including, but not limited to, Windows 2000, Windows NT 4.0, Solaris 2.X, HP-Unix, and Mac Operating System (OS)) and may host server as well as client applications and agents. Please note: systems referenced as examples in this definition may not qualify as candidate systems for transition to NMCI.

Certification. Within NMCI, the term "certification" refers to the process by which applications/systems are determined to be compatible with the NMCI network and its information assurance infrastructure. Thus, NMCI certification is a matter of system functionality within the enterprise network.

1.3 SEA ENTERPRISE ACTION BOD (SEA BOD) SERVER CONSOLIDATION AND REHOSTING

The Chief of Naval Operations (CNO WASHINGTON DC//N6F//191428Z Feb 04) has released guidance to the Navy regarding implementation of a strategy to address server consolidation and rehosting. In the Navy Information Technology (IT) environment, large numbers of legacy networks persist along side NMCI. This guidance provides the strategic overview of the Navy to leverage the integration of their functions into the NMCI infrastructure to eliminate to the absolute minimum a large number of legacy networks. The SEA BOD is directing multiple, related initiatives to improve the efficiency of Navy enterprise services management.

How this policy guidance will interface with the scope and processes contained in the LSTG have not been fully determined. When appropriate, specific information pertaining to SEA BOD will be incorporated into the guide.

1.4 ORGANIZATION OF THE LEGACY SYSTEMS TRANSITION GUIDE

The LSTG is organized to provide the readers (executive managers, supervisors, and technical staff) a guide that defines the approach and processes for transitioning legacy systems to the NMCI environment. The appendices provide reference materials, tools, and templates to assist in the transition process. Ideally, all readers would have the required time to read the entire LSTG. The authors of the LSTG realize, however, the resource of time is often scarce for many of the people intending to use the LSTG in the transition of their systems to the NMCI environment. The following Table 1-1 summarizes the intended primary audience for each section and appendix of the LSTG.

Table 1-1 LSTG: Intended Audience

Section	Intended Audience
1.0 BACKGROUND	Executive Managers, Supervisors, and Technical Staff
2.0 LEGACY SYSTEM TRANSTION PROCESS	Executive Managers, Supervisors, and Technical Staff
2.1 Legacy System Transition Team	Executive Managers, Supervisors, and Technical Staff
2.2 Provide Site Awareness	Supervisors and Technical Staff
2.3 Assess and Analyze Legacy System	Supervisors and Technical Staff
2.4 Order CLIN	Supervisors and Technical Staff
2.5 Develop Transition Plan	Supervisors and Technical Staff
2.6 Execute System Transition	Supervisors and Technical Staff
2.7 Conduct Post Execution Activities	Technical Staff
2.8 Resume Normal Operations and Maintenance and Life Cycle Management (C&A)	Technical Staff
3.0 C&A ACTIVITIES: APPROVAL TO TRANSITION TO NMCI	Supervisors and Technical Staff
4.0 CONCLUSIONS	Executive Managers, Supervisors, and Technical Staff
Appendix A: List of Resources	Supervisors and Technical Staff
Appendix B: Acronym List and Terminology	Executive Managers, Supervisors, and Technical Staff
Appendix C: SSAA	Technical Staff
Appendix D: CLIN 29 Request Package Template	Supervisors and Technical Staff
Appendix E: EDS CLIN Package Scenarios	Supervisors and Technical Staff
Appendix F: Legacy System Transition Team	Executive Managers, Supervisors, and Technical Staff
Appendix G: POA&M	Supervisors and Technical Staff
Appendix H: Risk Management Assessment Tool	Supervisors and Technical Staff
Appendix I: Team Responsibility Matrix	Executive Managers, Supervisors and Technical Staff
Appendix J: Project Milestones and Documentation Delivery Checklist	Executive Managers, Supervisors and Technical Staff
Appendix K: Coordination Appendix	Executive Managers, Supervisors and Technical Staff
Appendix L: Technical Reference Appendix	Technical Staff
Appendix M: PM Reference Appendix	Supervisors
Appendix N: Security Reference	Supervisors and Technical Staff
Appendix O: Cost Estimate Model	Executive Managers, Supervisors and Technical Staff
Appendix P: ST-ERQ	Supervisors and Technical Staff

2.0 LEGACY SYSTEM TRANSITION PROCESS

The Legacy System Transition Process provides the Site Representative, CDA, and PM with a method to successfully transition Legacy Systems into NMCI. Depicted in Figure 2-1, the Legacy System Transition Process outlines the high level processes and expected documentation required for each sub-process. For each high level process, a section of this guide is referenced and denotes where the sub-process is described in more detail. Although the Legacy System Transition Process is depicted in a traditional "waterfall" or sequential model, some activities and sub-processes may be planned to overlap and/or execute concurrently.

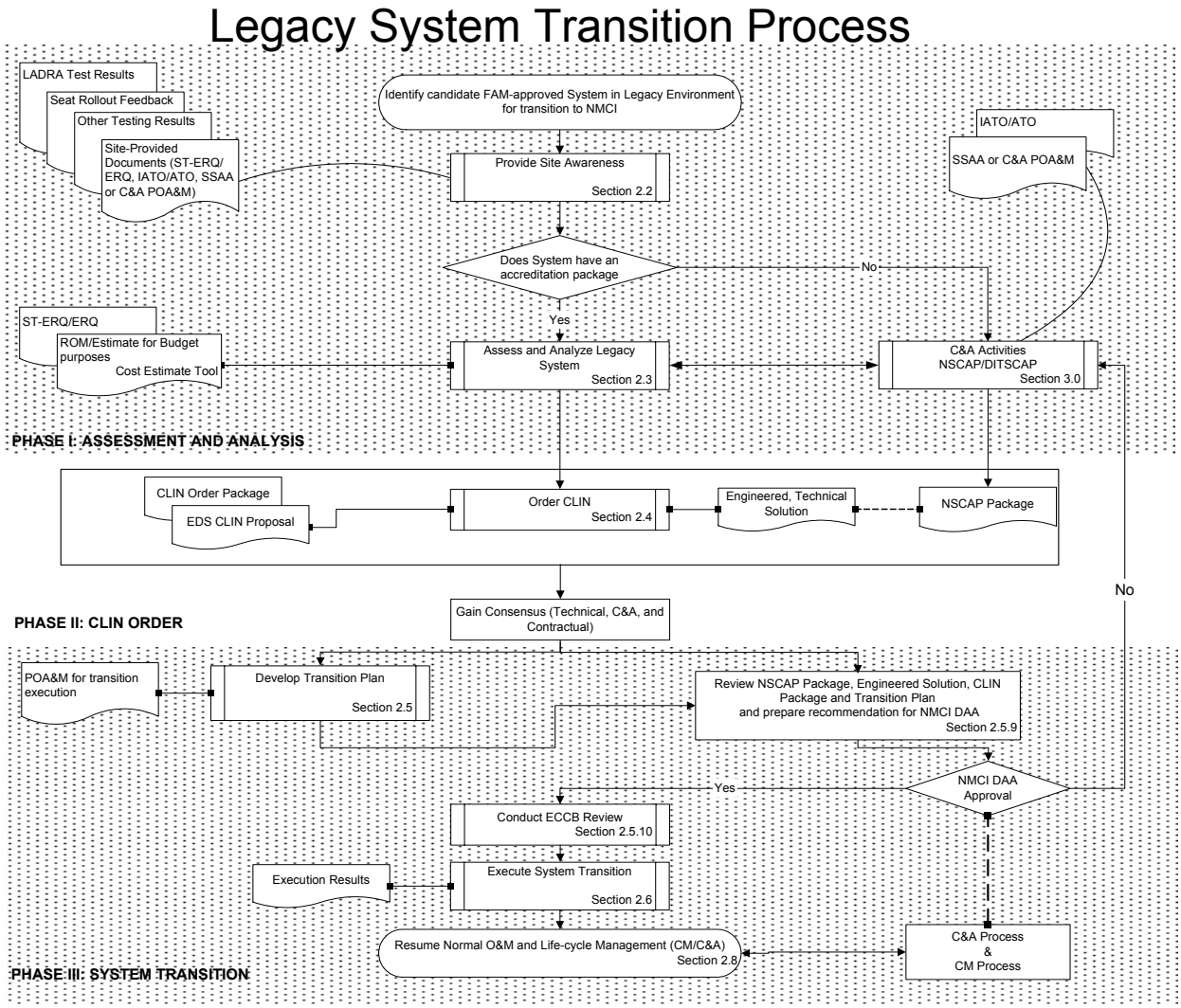


Figure 2-1 Legacy System Transition Process (High Level View)

A FAM-approved system is the fundamental entry criteria for any system to enter the NMCI transition process; hereafter a FAM-approved system is referred to as a candidate Legacy System or a candidate system.

Understanding a candidate Legacy System's current C&A status is an essential requirement prior to proceeding with any extensive transition planning efforts. If a candidate Legacy System does not have a complete accreditation package, the C&A processes will guide the Site Representative, CDA, and PM to attain accreditation and IATO or ATO (Interim Authority to Operate/Authority to Operate) prior to executing the System Transition.

All systems identified to transition to NMCI will be required to execute the NSCAP and produce the NSCAP package for DAA approval. DAA approval and ECCB approval are required prior to executing the System Transition. It should be noted that the NSCAP is complete for those systems that do not have an already existing DITSCAP. For those sites complete the NSCAP package is an initial document to achieve IATO and a complete DITSCAP is required following transition.

As Site Representative, CDA, and PM or quarantine remediation teams identify candidate systems to transition to the NMCI environment, a Site Awareness session will be conducted. Senior Navy officials, in conjunction with the FAM-approved list, determine the prioritization of candidate systems transitions. Prior to conducting Site Awareness, the Site Representative, CDA, and PM will assemble their currently available documentation: System Transition Engineering Review Questionnaire (ST-ERQ)/Engineering Review Questionnaire (ERQ), System Security Authorization Agreements (SSAA), and IATO/ATO. During the Site Awareness session the Legacy System Transition Process is introduced, tools to assist in preparing CLIN Order Packages and ROM/budget estimates are provided, and the required documentation is reviewed and updated as necessary. Please refer to Appendix O for ROM/budget estimates information.

After the Site Awareness session is complete and required documentation is updated, the candidate Legacy System is assessed and analyzed in the context of transitioning to the NMCI environment.

The results of the assessment and analysis directly contribute to identifying a recommended high-level solution and preparing the CLIN Order Package. Once the Site Representative, CDA, and PM have submitted a CLIN Order Package, the EDS Business Office receives it and assesses the package. After the EDS Business Office completes its assessment of the CLIN Order Package, the EDS Business Office prepares a proposal and submits the proposal with an Engineered Technical Solution. Finalizing the CLIN Order Package with the NSCAP is an iterative process that requires consensus among all technical, C&A and contractual participants. The Site Representative, CDA, and PM review EDS's proposal and Technical Solution; if the Site Representative, CDA, and PM accept the proposal and Technical Solution, the Transition Plan is developed specific to the candidate Legacy System.

During the development of the Transition Plan, the resources and responsibilities are identified for each milestone. Additionally, the NMCI environment, the Legacy System, and its supporting systems are prepared for transition, test plans are completed, and training is conducted. The Transition Plan includes the Plan of Action and Milestones (POA&M), System Operational Verification Test (SOVT), Test Plans, and additional required documentation.

After completing all Transition Plan development activities and completing all coordination activities, the system is transitioned to the NMCI environment. Capturing all execution results and documenting any issues can quantitatively assess the system for resuming normal operations and maintenance or reverting back to the legacy environment.

2.1 PROVIDE SITE AWARENESS

The objective of this phase is for the IATT to educate and advise the Site Representative, CDA, and PM on the process by which Legacy Systems are transitioned to NMCI. The IATT personnel working in support of the site will provide initial site overview to the NMCI transition process and support the site

with continuity throughout the Legacy System Transition Process. Site Awareness is typically the first opportunity for the site to receive an introduction to the Legacy System Transition Process and the tools, templates, and guidelines associated with the process.

The IATT will review the completed pre-Site Visit documentation and brief all of the concerned parties on the items that will be required to proceed into the System Assessment and Recommended Technical Solution phase of the System Transition. The IATT personnel will assist the Site Representative, CDA, and PM in using the decision tools to ultimately prepare the CLIN Order Package. When appropriate the EDS Base Operations will assist the IATT by advising the Site Representative, CDA, and PM of the potential System Placement and CLIN Order options described in the decision tools. The IATT C&A personnel will provide an overview of the NSCAP and all other C&A processes (i.e. introduction, submittal process, general guidance). The C&A personnel will also assist in gathering the required/available C&A documentation. These roles are illustrated in Figure 2-2.

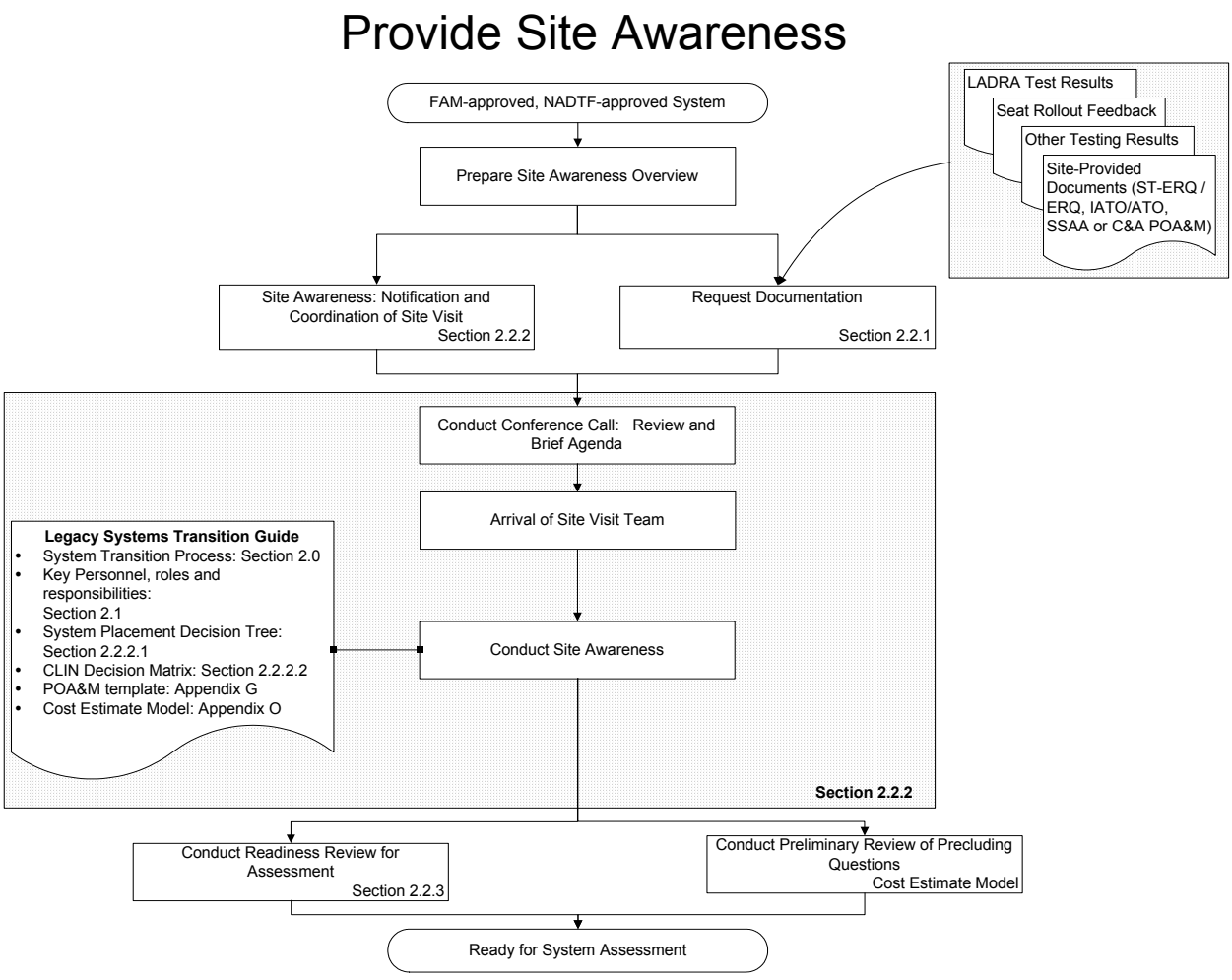


Figure 2-2 Provide Site Awareness

2.1.1 Request Documentation

The EDS Business Office, the IATT, CDA, and PM may assemble any documents outlined below prior to the initial site visit. Understanding the required documents may not be tailored to the Legacy System Transition Process, the IATT personnel supporting the site will provide an overview of the unique requirements associated with each document as it is related to the Legacy System Transition Process. Final delivery of the required documents will be expected at the completion of the System Assessment Phase.

1. Engineering Review Questionnaire (ERQ): The ERQ is a document designed to collect information that will be used in analyzing a system's requirements and configuration to determine how to best transition the system to NMCI, and in completing the ST-ERQ. By using the ERQ template, all information is presented to the System Analysis Team and the EDS Business Office in a standardized format, which allows each organization to streamline their processes. If the ERQ has not been completed or updated, the Site Representative, CDA, and PM must complete the ST-ERQ in lieu of the ERQ.

    a. System Transition Engineering Review Questionnaire (ST-ERQ): The ST-ERQ is a document specifically designed for the Legacy System Transition Process to collect information that will be used in analyzing a system's requirements and configuration to determine how to best transition the system to NMCI. The ST-ERQ is required to develop a Recommended Technical Solution.

2. System Security Authorization Agreement (SSAA): The SSAA is a description of the system mission, target environment, target architecture, security requirements, and applicable data access policies. It also describes the applicable set of planning and certification actions, resources, and documentation required to support the certification and accreditation. It is the vehicle that guides the implementation of INFOSEC requirements and the resulting certification and accreditation actions. (DoD Instruction Number 5200.40) If a system does not have a SSAA then the site may choose to use the rapid accreditation process defined in the NSCAP to develop a C&A POA&M. The ultimate goal is for the system to attain a DITSCAP-compliant SSAA.

3. Interim Authority to Operate/Authority to Operate (IATO/ATO): The ATO or IATO for systems and applications requesting connection to NMCI must be supported with information identifying and describing the residual risks that will be assumed by the NMCI and accepted by the Navy NMCI DAA.

Often Legacy Systems will have other useful documents that contain more detail or support the ST-ERQ/ERQ, SSAA, or IATO/ATO. Additional useful documents include the checklist provided in Table 1, Section 4.2 of the NSCAP and other example documents listed below:

1. Concept of Operations (CONOPS)
2. System Architecture/Design Document
3. Security Architecture Documentation
4. Integrated Logistics Support Plan (ILSP) or other Configuration Management documentation
5. User Logistics Support Plan (ULSP) or other Configuration Management documentation

2.1.2 Site Awareness: Notification and Coordination of Site Visit

The objective of the Site Awareness phase is to educate and advise the Site Representative, CDA, and PM on the process by which Legacy Systems are transitioned to NMCI. Notification and coordination activities associated with the Site Visit are described below.

Approximately two to three weeks prior to the projected arrival for the initial site visit, the team leader will notify the Site Representative, CDA, PM, and all concerned, identifying the names and contact data for the key visiting team personnel, the team leader, pertinent directives or correspondence affecting that particular team visit, and a proposed date for the Site Visit. The Planning and Coordination Team will also request that pre-Site Visit documentation be sent from the Site Representative, CDA, and PM to the key visiting team personnel.

Approximately one week prior to the group's arrival, the team leader will schedule a conference call for all personnel involved in the System Transition to facilitate the arrival and introduction of the IATT personnel and coordinate the In-Brief. The IATT personnel will review the pre-Site Visit documentation previously received from Site Representative, CDA, and PM. Two business days prior to the arrival of the Site Visit Team, the team leader will present a proposed agenda for the In-Brief and recommended audience. The agenda will include the following:

- Provide an overview of the System Transition Process.
- Review C&A processes.
- Review the CLIN Decision Matrix.
- Review System Placement Decision Tree.
- Discuss Site System Transition Milestones.
- Identify Key Personnel (PMO, EDS, Site Representative, CDA, and PM, etc.).
- Define Transition Responsibilities.
- Define Reporting Responsibilities.
- Review NMCI Enterprise Network Architecture.
- Review Risk Assessment Tools.
- Solution Options

The recommended audience may include the following: Site Representative, CDA, PM, Site C&A Team, EDS Base Operations, and Site/System technical staff (system administrators, database administrators, system security administrators, network administrators, developers, facilities management, etc.).

2.1.2.1 System Placement Decision Tree

The System Placement Decision Tree is an analysis tool that assists each Site Representative, CDA, and PM to determine where the Legacy System should reside within NMCI. The Decision Tree, depicted in Figure 2-3, identifies all of the criteria that must be analyzed to determine whether the Legacy System should be transitioned to the NMCI Trusted Enclave or to the NMCI DMZ (Demilitarized Zone). A thorough analysis of the Decision Tree is critical to the successful transition of Legacy Systems.

In accordance with the Decision Tree, the first criterion that must be determined is whether the system is/was being designed for DON users within NMCI. If the system is not being designed for NMCI users these requirements do not apply.

Once it is determined that these criteria apply, the Site Representative, CDA, and PM should then ensure the appropriate "application" or "system" level DITSCAP Accreditation is available. If a determination

regarding the correct DITSCAP Accreditation cannot be made, please contact the PMO Systems Transition Team for guidance.

The next step is to determine the system users. If only NMCI users require access to the system it is recommended that the system be transitioned to the NMCI Trusted Enclave. If non-NMCI users also require access to the system the Site Representatives, CDA, and PM should consult the Unclassified Trusted Network Protection Policy (UTNPP) to determine whether the system is compliant. Unclassified sections of the latest NEPP are located at https://infosec.navy.mil/ under Fleet Documents (this includes the list of approved, non-compliant apps/ports/protocols and services allowed, and for how long). The entire policy can be found at https://infosec.navy.smil/mil. If the system is compliant it should be transitioned to the NMCI Trusted Enclave. If the system is not compliant the system must be transitioned to the NMCI DMZ.

Finally, once the System Transition location is identified, the Site Representative, CDA, and PM should refer to the CLIN Decision Matrix to assist in determining the appropriate CLIN requirement necessary to complete the CLIN Order Package.

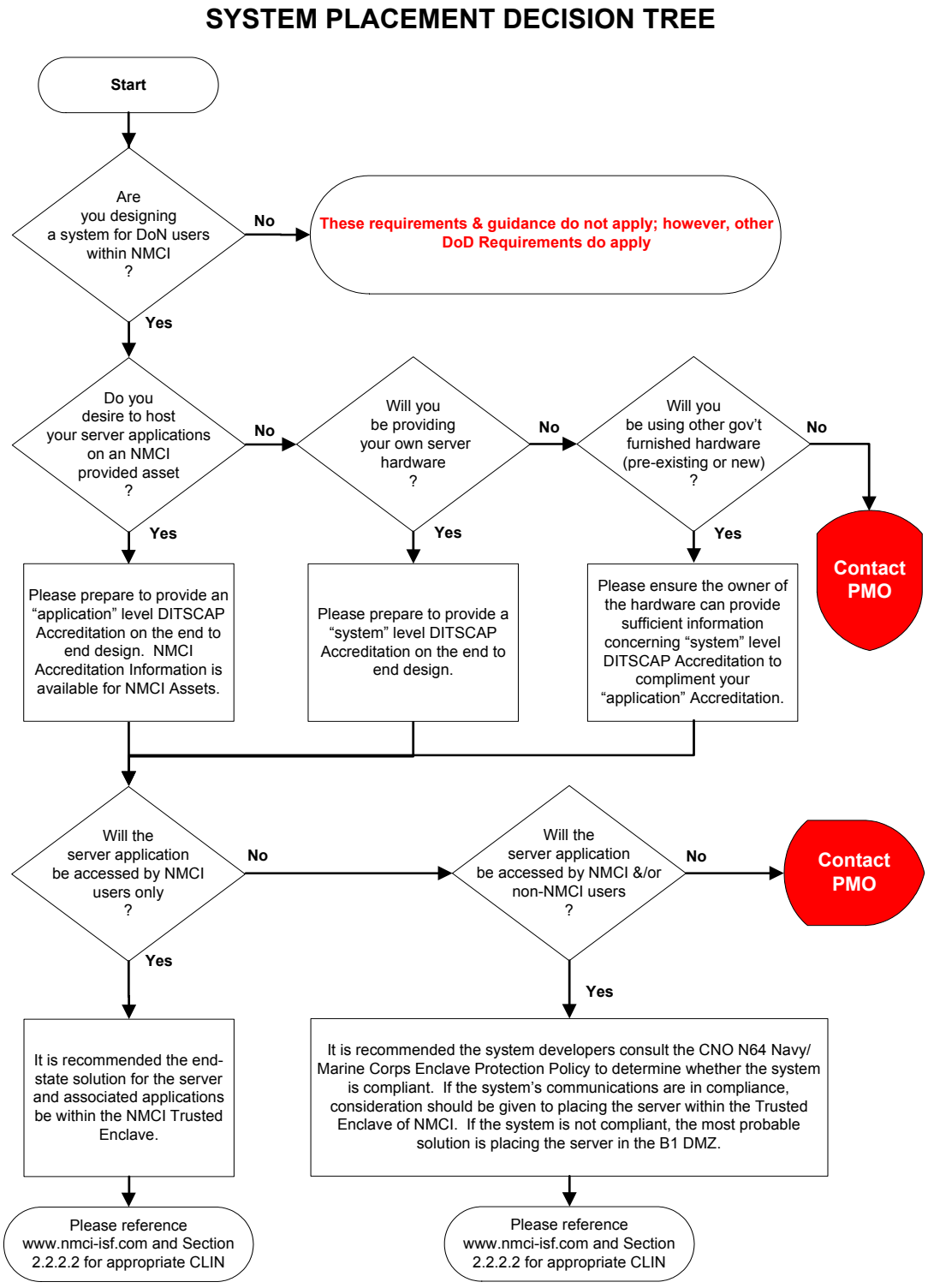


Figure 2-3 System Placement Decision Tree

2.2 CUSTOMER LINE ITEM NUMBER (CLIN)

NMCI service offerings, commonly referred to as CLINs, features online and downloadable versions of the NMCI CLIN catalog, which provides a description of individual service offerings, associated Service

Levels, software, hardware and pricing, as applicable. Where pictures and specifications are provided with CLIN service descriptions, the actual CLIN item delivered may be different from what is shown or listed. These substitutions or changes may result from technology insertions, model or production changes or other changes in technology.

2.2.1 CLIN 0006 Additional Wall Plug Service

This service provides access to the NMCI network in the form of a wall plug, which allows direct, local connectivity to NMCI in accordance with the security requirements, and policies of the NMCI contract. This item is only required when there is not an existing NMCI wall plug available to support connectivity of the server to the NMCI network.

Additional information regarding this item is available at the following link: http://www.nmci-eds.com/clin006.htm.

2.2.2 CLIN 0027AA - AC Standard Bandwidth Application

Application server connectivity is a service that provides NMCI connectivity to legacy application servers for Navy and Marine Corps organizational, operational, and functional applications to meet mission requirements. This service will meet peak network loading requirements of users for replication, but does not include server and database maintenance and administration. This option provides a standard level of support for availability, network loading, and maintenance responsiveness.

There are three (3) version of this CLIN to select from:

- CLIN 0027AA – Standard Low Bandwidth Application (10 Mbps)
- CLIN 0027 AB – Standard Medium Bandwidth Application (100 Mbps)
- CLIN 0027AC – Standard High Bandwidth Application (1 Gbps)

This item covers connectivity for application servers above and beyond the 2,100 legacy applications included as a part of the NMCI basic service. This item provides a single static IP address and supports connectivity to application servers that are added to the network after establishment of baseline services.

Additional information regarding this item is available at the following link: http://www.nmci-eds.com/clin027aa.htm.

2.2.3 CLIN 0027AD - AF Mission-Critical Bandwidth Application

Provides connectivity between an application server and the network backbone of the local supporting backbone. Provides an increased level of availability, reduced network loading and greater maintenance responsiveness a two static IP addresses for redundancy.

There are three (3) version of this CLIN to select from:

- CLIN 0027AD – Mission-Critical Low Bandwidth Application (10 Mbps)
- CLIN 0027AE – Mission-Critical Medium Bandwidth Application (100 Mbps)
- CLIN 0027AF – Mission-Critical High Bandwidth Application (1 Gbps)

Additional information regarding this item is available at the following link: http://www.nmci-eds.com/clin027ad.htm.

2.2.4 CLIN 0027AG Legacy Application server Connection

Application server connectivity is a service that provides NMCI connectivity to 2100 (1500 for Navy and 600 for Marine Corps) legacy applications that are included as a part of the NMCI basic service. The decision regarding the 1500 applications will be made upon completion of a more complete analysis. Urgent near term requests for the use of this CLIN should be directed to applicable FAM and Director, NMCI.

Additional information regarding this item is available at the following link: http://www.nmci-eds.com/clin027ag.htm.

2.2.5 CLIN 0029 Legacy Systems Support

Legacy Systems Support provides initial integration services for emerging operational and functional systems to enable them to run on NMCI. Legacy system support can also provide additional services beyond basic integration. These additional services provide a range of options that include, but are not limited to, NMCI EDS hosting of applications, operations and maintenance support, database management, and training, if ordered. This service may include participation of EDS in business process re-engineering activities.

Additional information regarding this item is available at the following link: http://www.nmci-eds.com/clin029.htm.

2.3 CLIN DECISION MATRIX

As referenced in the System Placement Decision Tree, the CLIN Decision Matrix below is designed to help in determining the appropriate CLIN 27 and CLIN 29 requirements. If other CLIN solutions are required, please refer to http://www.nmci-eds.com/clinlist.htm. Prior to the arrival of the System Assessment Team, the Site Representative, CDA, and/or PM must select the appropriate case number identified below. A completed ST-ERQ/ERQ significantly contributes to the CLIN decision process. By ascertaining the decision criteria outlined in the CLIN Decision Matrix, the preliminary approach to CLIN selection and Technical Solution directly contributes to the development of the CLIN Order Package.

Table 2-1 CLIN Decision Matrix

Case	Hardware/ Operating System provided by	Application Software provided by	Hardware/ Operating System managed by	Application Software managed by	Connection	CLIN Requirement
Case 1	EDS	EDS	EDS	EDS	EDS	CLIN 29
Case 2	Government	EDS	EDS	EDS	EDS	CLIN 29
Case 3	EDS	EDS	EDS	Government	EDS	CLIN 29
Case 4	EDS	EDS	Government	Government	EDS	CLIN 29
Case 5	EDS	Government	EDS	Government	EDS	CLIN 29
Case 6	Government	Government	EDS	EDS	EDS	CLIN 29
Case 7	Government	Government	EDS	Government	EDS	CLIN 29
Case 8	EDS	Government	Government	Government	EDS	CLIN 29
Case 9	Government	Government	Government	Government	EDS	CLIN 27

Per the matrix above, the Government or EDS are the only two entities that can provide the above services. The Government can include civil servants or civilians, military personnel, and/or non-EDS contractors. As shown in Table 2-1, multiple cases exist with EDS hosting services. For example, in Case 4 EDS provides the hardware and software platform hosted at the data center; however, the appropriate Navy system and data owner perform administration of the system and application. In Case 6, the government provides the hardware and software platforms to the data center where EDS personnel perform local administration of the hardware, operating system, and application.

EDS is currently developing scenarios for the cases identified above. These scenarios will be added to Appendix E of this document once they are completed.

If the Site Representative, CDA, and PM select EDS supporting services or EDS Hosting services (Cases 1-8), which include providing or managing hardware, operating systems, and/or application software, the Site Representative, CDA, and PM will be required to submit a CLIN 29 package. The case selected in the Decision Matrix will determine what needs to be included within the CLIN 29 package.

If the Site Representative, CDA, and PM do not request supporting or hosting services the Site Representative, CDA, and PM will be required to submit a CLIN 27 package (Case 9).

2.3.1 Readiness Review for System Assessment

The objective of the Readiness Review is for Site Visit Team to recap the transition process and review the site/system's current state as it applies to System Assessment. Consequently, the Readiness Review covers the following:

- Review current accreditation package.
- Identify any actions required to schedule the System Assessment.
- If applicable, schedule System Assessment.
- Introduce the Planning and Coordination Team POC.
- Identify key technical personnel representing the Site Representative, CDA, and PM, and System Transition Team who will be interfacing with the IATT.

2.4 ASSESS AND ANALYZE LEGACY SYSTEM

Assessing the Legacy System provides the IATT with a realistic understanding of the current system configuration, security status, and system architecture. Analyzing the Legacy System provides quantitative tools and guidelines to develop a Recommended Technical Solution. This process is depicted in Figure 2-4. As the work product of this phase, the Recommended Technical Solution directly contributes to the preparation of the CLIN Order Package.

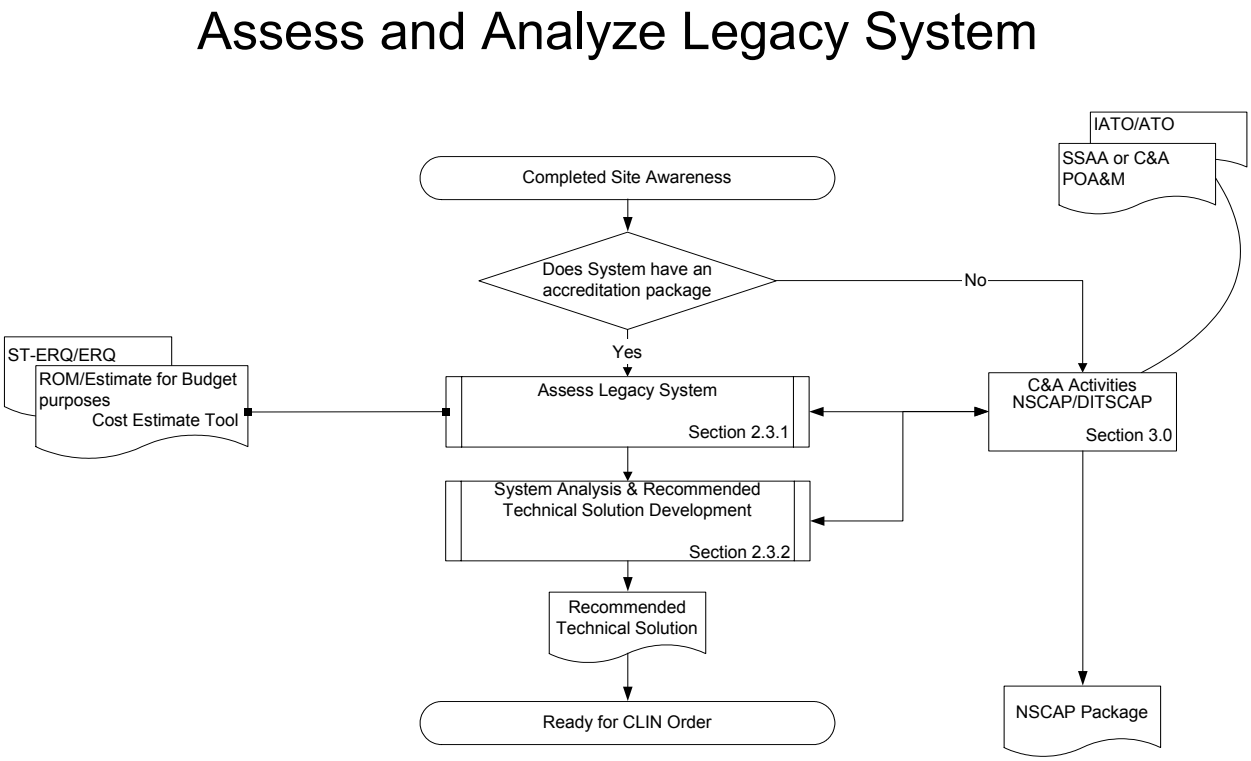


Figure 2-4 Assess and Analyze Legacy System

2.4.1 Assess Legacy System

During the System Assessment phase of the System Transition, the Team Leader will work with the technical personnel to complete documentation gathering, consolidate and capture the information associated with the "As-Is" system, and verify the system's C&A status. To complete this phase, IATT personnel will use the results from the Site Visit, and physical Site Survey, as well as information collected from a system requirements review and a technical assessment of the production and supporting systems. This process is depicted in Figure 2-5.

The completed System Assessment will include a detailed summary from the physical site review, system requirements review, technical system assessment, supporting/interfacing systems technical assessment, and mission/policies review. A review will also be conducted of the completed pre-Site Visit documentation for any discrepancies and assist the Site C&A Team, Site Representative, CDA, and PM in completing these documents so they can be used during development of the Recommended Technical Solution. The results of the System Assessment will directly contribute to the development of the Recommended Technical Solution and subsequently the finalization of the CLIN Order Package.

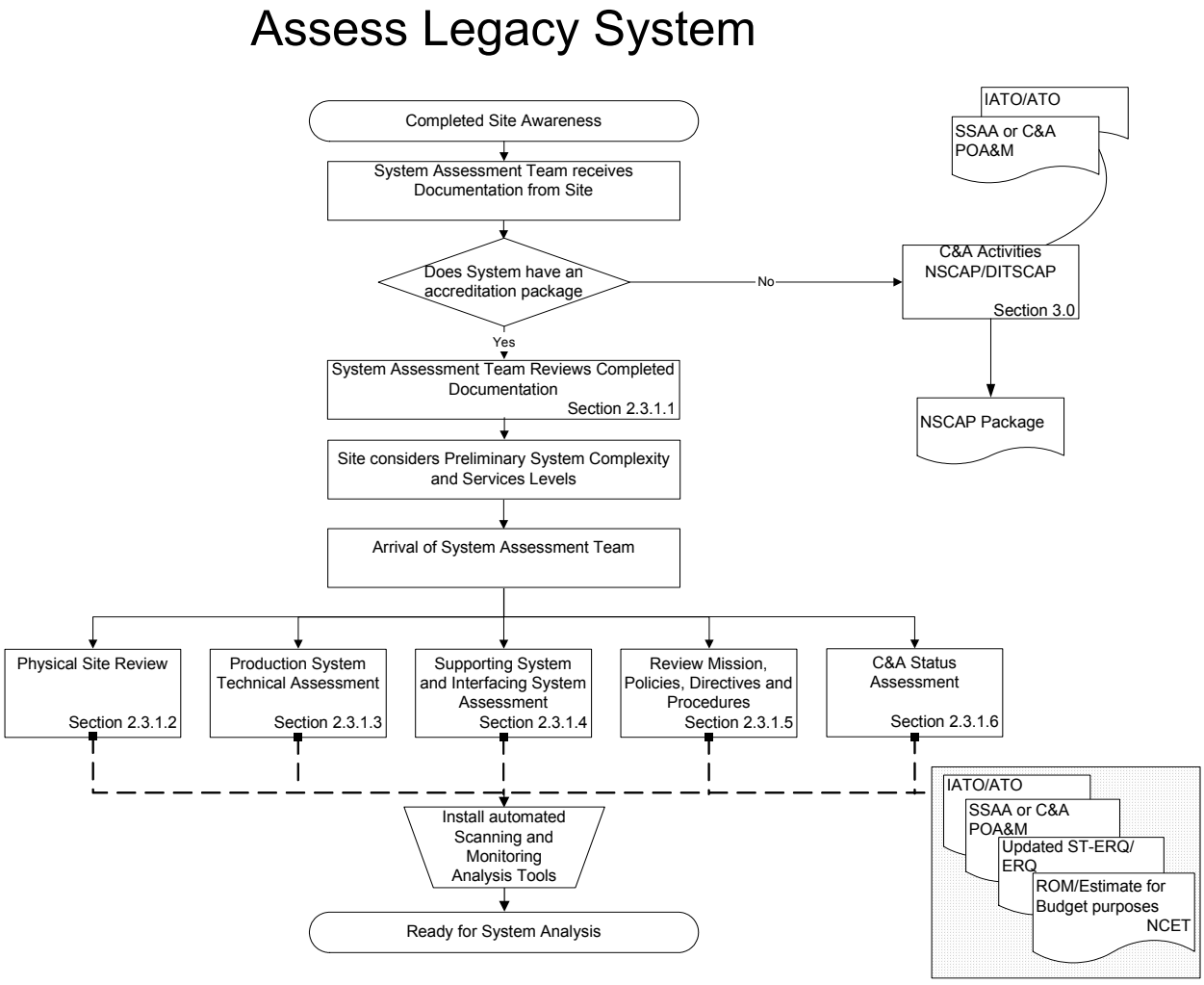


Figure 2-5 Assess Legacy System

2.4.1.1 Review Completed Documentation

In this phase, the IATT will review the three documents listed below and any supplemental documentation. The Site Representative, CDA, PM, and IATT will identify and communicate gaps, areas requiring clarification, and potential errors upon reviewing the documentation. Additionally, the Site Representative, CDA, and PM, and the IATT must complete the ST-ERQ, using the information gathered during the System Assessment. The ST-ERQ will provide the system-specific information required to develop a Recommended Technical Solution.

1. ERQ: A document designed to collect information that will be used in analyzing a system's requirements and configuration to determine how to best transition the system to NMCI and in completing the ST-ERQ.

    a. System Transition Engineering Review Questionnaire (ST-ERQ) – The ST-ERQ is a document specifically designed for the Legacy System Transition Process to collect information that will be used in analyzing a system's requirements and configuration to

determine how to best transition the system to NMCI. The ST-ERQ is required to develop a Recommended Technical Solution.

2. SSAA: The IATT C&A personnel will review the DITSCAP compliant SSAA verifying the system mission, target environment, target architecture, security requirements, and applicable data access policies. The Site, CDA, and PM will use the DITSCAP compliant SSAA as a vehicle to guide the implementation of INFOSEC requirements and the resulting certification and accreditation actions. [DoD Instruction Number 5200.40]

3. IATO/ATO: The IATO or ATO for systems and applications requesting connection to NMCI must be supported with information identifying and describing the residual risks that will be assumed by the NMCI and accepted by the Navy NMCI DAA. Although a system may have an existing IATO or ATO, the risks associated with the system transitioning to NMCI may differ, thus requiring an updated IATO or ATO prior to transitioning the system to the NMCI environment.

2.4.1.2 Physical Site/Facilities Review

The objective of this phase is to conduct a detailed physical Site Survey to identify the existing environmental conditions to mitigate any risk associated with the transition and ongoing support of the System, and to identify any preparation work that will be required to ensure the environment will be ready to accept the transitioned system.

While conducting the physical Site Survey, the IATT, Site Representative, CDA, and PM should complete an inventory audit and an environmental analysis consisting of the following:

- Security Analysis (ex: security and monitoring policies, 24/7/365)
- Reliability (ex: power protection, uninterruptible power supply (UPS))
- Redundancy (ex: connections)
- Rack space
- Heating, ventilation, and air-conditioning (HVAC)
- Other as required

Once the audit and analysis are complete, the IATT will work with the Site Representative, CDA, and PM to document and diagram the results in the ST-ERQ (please refer to Appendix L).

2.4.1.3 Production System Technical Assessment

In assessing a Legacy System for transition to the NMCI environment, the IATT will request the Site Representative, CDA, and PM to assist in capturing the following technical information which will be documented in the ST-ERQ:

- Depict the system architecture in graphical form and provide a brief description of each sub-system/component.
- Summarize each system's configuration or current baseline information including the following: hardware platform, operating system with version and service pack or patch level, commercial off-the-shelf (COTS) products with service pack or patch level, network connections (with Internet Protocol (IP) address and subnet mask), and any peripherals.
- Determine system transition impact on client configuration.

- Describe the production system noting all applications, application version or build number, system availability requirements, average downtime, and user community (reference engineering questionnaire).
- Describe the complexities associated with this system (numerous interfacing systems, minimal documentation, multiple-tier architecture, old/non-supported hardware or software, non-Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, etc.).
- Describe the non-production systems that are required to support the production system—development and/or testing systems.

2.4.1.4 Technical and Programmatic Information

The below listed information will be useful in completing the System Assessment and provides a more complete picture of the system as it functions in production:

- Using the information from the System Assessment as the baseline, prepare a detailed diagram and inventory of the entire system (include all hardware, network connections, security/encryption/firewalls, operating systems, middleware, legacy applications, etc.).
- Describe any scheduled system activities (i.e., batch jobs, cron jobs, archive activities, etc.).
- Include the current system schedule for maintenance upgrades or patches for the transitioning system and any relevant supporting or interfacing systems.
- Describe any assumptions, issues, and/or concerns associated with transitioning this Legacy System to the NMCI Base Area Network (BAN) or Enclave.

2.4.1.5 Supporting Systems and Interfacing Systems Technical Assessment (development, test, integration environments)

Supporting and Interfacing Systems often provide or support mission critical requirements or system requirements. The objective in assessing these systems and their functions in relation to the transitioning system is often the discriminating factor for planning and executing system transitions. Results from performing this technical assessment will be captured in the ST-ERQ. Examples of supporting systems or interfacing systems follow:

- Backup systems
- Print servers
- Test servers
- Integration systems
- Voice Response Unit (VRU) interface
- Development systems
- Interfacing systems
- Fax/Scanning systems
- Security systems (firewalls, tripwire, monitoring systems)
- Off-line storage systems (optical drives, RAID, etc.)
- External devices (unique tape drives)

2.4.1.6 Review the Mission, Policies, Procedures, and Directives associated with the System and its Interfacing Systems

Often government/DoD systems have specific configuration, functionality, or performance requirements that do not directly correspond to the technical aspects of a system. A mission constraint, directive,

policy, or law may be the source of the technical configuration. Consequently, this section of the document serves as a reminder to the Site Representative, CDA, and PM to call out specific policies, procedures, directives, or mission requirements during the System Assessment phase.

2.4.1.7 C&A Status Assessment

The IATT Team Leader and technical members will assess the system's current C&A status by comparing the data collected to the checklist in Section 4.2 of the NSCAP. SSAA and the site IATO/ATO will also be reviewed.

If the "As-Is" system has not been granted an IATO/ATO and has not obtained a signed and completed DITSCAP-compliant SSAA, a C&A POA&M will be prepared with the site that when successfully executed gains the system accreditation for both "As-Is" and NMCI environments.

If the "As-Is" system has been granted an IATO/ATO and has obtained a signed and completed DITSCAP-compliant SSAA, the IATT will prepare a NMCI C&A POA&M which directly assists the Site Representative, CDA, and PM in completing the NSCAP Package and obtaining Navy NMCI DAA approval.

Section 4 of the NSCAP provides detailed information regarding the C&A Assessment.

2.4.2 System Analysis and Recommended Technical Solution Development

The System Analysis and Solution Development Team performs the analysis of the Legacy System, depicted in Figure 2-6, which includes data sufficient to enable the Site Representative, CDA, and PM to complete the Recommended Technical Solution and SSAA or C&A POA&M. The Certification Agent Team and the Site C&A Team provide C&A guidance in the development of the Recommended Technical Solution. The System Analysis efforts and Recommended Technical Solution will directly contribute to the development of the CLIN Order Package.

The IATT initial technical analysis will consider the following:

- Review the completed ST-ERQ.
- Review system information including initial-state network diagram.
- Analyze existing documentation gathered during the Site Visit and System Assessment.
- Analyze output of the System Placement Decision Tree and the CLIN Decision Matrix.
- Analyze impact of Client Seats.

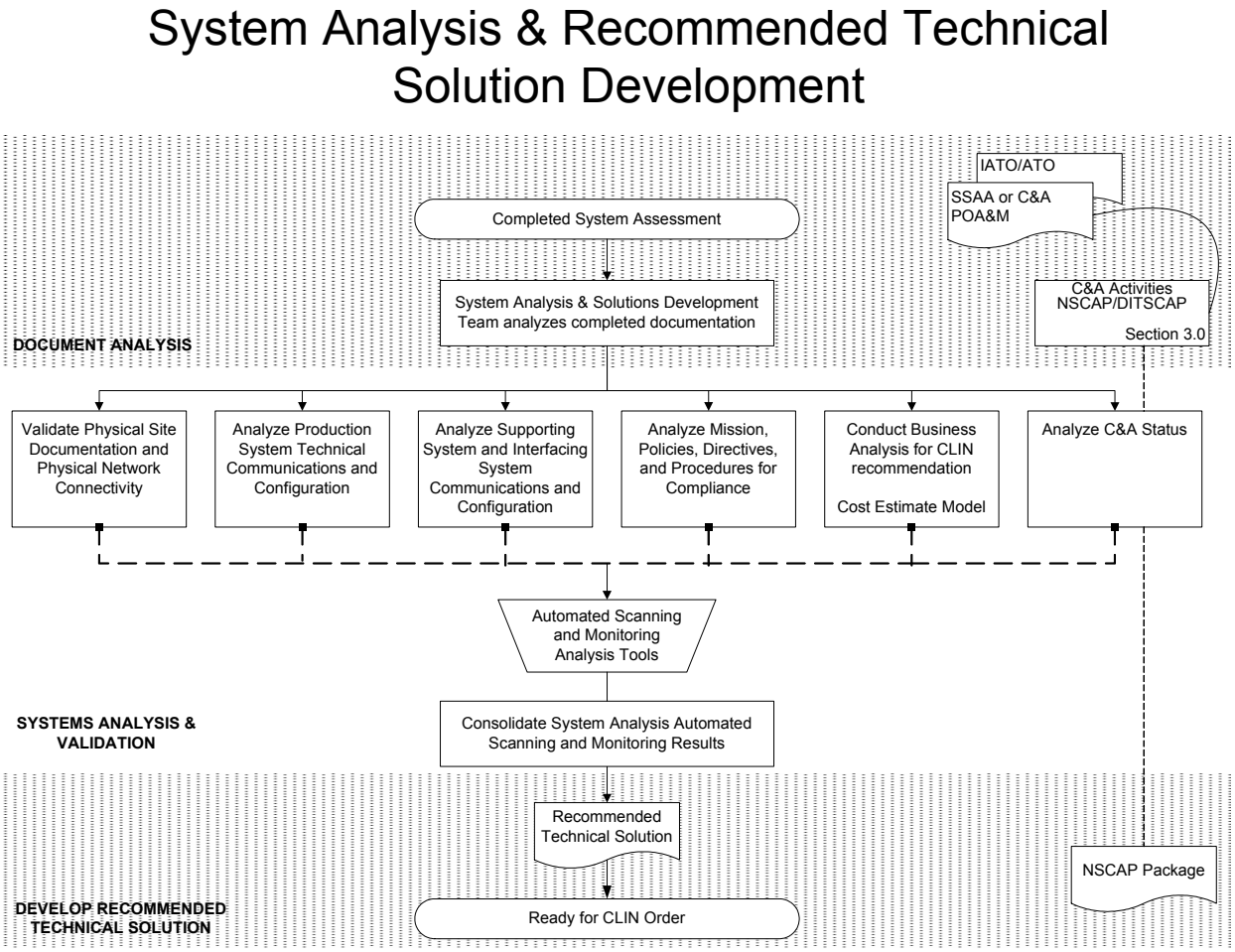


Figure 2-6 System Analysis & Recommended Technical Solution Development

2.4.2.1 Document Analysis

During System Assessment and Technical Solution Development, the IATT will work with the Site Representative, CDA, and PM to identify the current and future system requirements, as appropriate, that must be included in the Recommended Technical Solution. Understanding the system requirements is a primary component of documentation analysis. The following system requirements should be considered in conducting documentation analysis:

- Reliability:
  - Redundant or self-healing network connection.
  - Hardened physical facilities (e.g. redundant HVAC and power, layered security, intrusion detection, 24x7x365 management and monitoring, and guaranteed repair intervals)

- Redundancy:
  - Redundant servers (systems and locations)
  - Clustering
  - Managed storage services (e.g. tape backups)

- Failover:
  - Managed load balancing
  - Managed database services

- Recovery:
  - Managed storage (e.g. tape backups and data recovery)
  - Managed load balancing (e.g. physical facilities)

- Synchronization:
  - Tape restoration
  - Clustering
  - Database replication and mirroring

- Bandwidth:
  - Capacity planning (considering User to Application Mappings (UTAM), Replication, Synchronization, and Load Balancing)

- System Security:
  - Firewalls
  - Data integrity (intrusion detection, tripwire, or similar products)
  - Hardening scripts
  - Confidentiality/Integrity (Access Control lists and Authentication)
  - Encryption requirements

- Management and System Administration:
  - Console
  - R/W/B seat (no root access required)
  - S&T seat (CLIN 38)

2.4.2.2 Systems Analysis and Validation

During Systems Analysis and Validation the IATT will conduct a thorough analysis of each candidate legacy system, considering the following while working to establish an appropriate technical solution:

- Validate physical site documentation and physical network connectivity
- Analyze production system technical communications and configuration
- Analyze supporting system and interfacing system communications and configuration
- Analyze mission, policies, directives, and procedures for compliance
- Conduct business analysis for CLIN recommendation (Cost Estimate Model)
- Analyze C&A status

With the results of the automated scanning and monitoring tools, the IATT will validate the network configuration, system communications, and security posture.

Additionally, each system has technical system constraints that may be applicable in analyzing the system's ability to transition. Technical constraints often influence the planning and development of a Technical Solution. The IATT will review and analyze technical system constraints in support of developing a Technical Solution. Examples include:

- Describe any assumptions, issues, and/or concerns associated with the end-state configuration or architecture.
- Assess the Legacy System's physical constraints (location, hardware, network infrastructure) as they relate to transitioning to the NMCI network.
- Describe any system or application instances where network information (IP addresses, domain server (DNS) names, etc.) is hard coded or defined in tables.
- Describe any potential data issues.
- Describe any variations from NMCI requirements/rules.
- If applicable, describe the technical constraints associated with EDS/NMCI server hosting/maintenance.
- Describe any system functions that may not move with the system (i.e. backups, interfacing systems' connectivity, and other maintenance functions).
- Describe the supporting systems' (testing/development, interfacing systems, or simulators) end-state configuration and required modifications associated with transitioning the Legacy System.
- Identify or define any changes to regularly scheduled activities (batch jobs, cron jobs, etc.) for the system.
- If applicable, describe any network/IP address and subnet mask modifications.
- If applicable, describe any physical relocation constraints (duration of downtime, geographic relocation constraints, data center constraints, etc.).
- Describe any hardware, software or maintenance agreement changes/upgrades required by System Transition.
- Categorize and prioritize the System Transition activities based on true availability and mission requirements.

2.4.2.3 Develop Recommended Technical Solution

The ultimate work product of the Assess and Analyze Legacy System phase is to recommend a Technical Solution that takes into account all of the results of the assessments conducted above and the results of the Site Visit. Also, the IATT will work in conjunction with the site to provide a system recommendation for enterprise review to facilitate the enterprise-wide solution. Often enterprise-wide solutions include reducing the number of applications, consolidating servers, and reducing facility space by co-locating servers.

The Technical Solution should include the following:

- Focus on Enterprise Solutions
- Identification of Key Personnel.
- Progress Tracking Document containing a planned progress.
- C & A documentation.
- Network diagrams (Initial-State diagram, Transition-State diagram, and End-State diagram).
- CLIN Order Package (outlined in Section2.5).
- Follows the framework as identified in the NRDDG.

The IATT will assist the Site to complete the three required documents (IATO/ATO, SSAA, and ST-ERQ) and Recommended Technical Solution and maintain a repository.

The IATT will serve as a liaison to the Site Representative, CDA and PM for Recommended Technical Solution prior to CLIN Order.

2.5 ORDER CLIN

The Site Representative, CDA, and PM order a CLIN for transitioning their system to the NMCI environment according to the guidelines outlined in the NMCI contract. The IATT will assist the Site Representative, CDA, and PM to ensure that the CLIN Order Package includes the Recommended Technical Solution requirements. The Order CLIN phase provides the Site Representative, CDA, and PM with high-level criteria for requesting services for candidate systems transitioning to NMCI. Technical decisions are often influenced by the business and cost constraints levied on the systems. Consequently, the Order CLIN phase provides a guide for the Site Representative, CDA, and PM to incorporate technical, business and financial decisions into the Legacy System Transition Process. As a result of this collaboration, the EDS Business Office develops a proposal that documents the Technical Solution and identifies any required costs.

The Site Representative, CDA, and PM review EDS's proposal and assess the Technical Solution and associated cost. As a result of the assessment, the Site Representative, CDA, and PM accept or decline EDS' proposal. If the Site Representative, CDA, and PM accept the EDS proposal, the Site Representative, CDA, and PM will finalize the Engineered Technical Solution and can proceed to develop the Transition Plan. If the Site Representative, CDA, and PM decline the EDS proposal, then the Site Representative, CDA, PM, and the EDS Business Office will work cooperatively to redefine the Technical Solution and associated cost. The CLIN Order Process is depicted in Figure 2-7.

Currently, the business decisions defining no-cost CLIN 27 criteria are not finalized. Therefore, future versions of the LSTG will incorporate no-cost CLIN 27 criteria decisions and any additional CLIN definition updates.

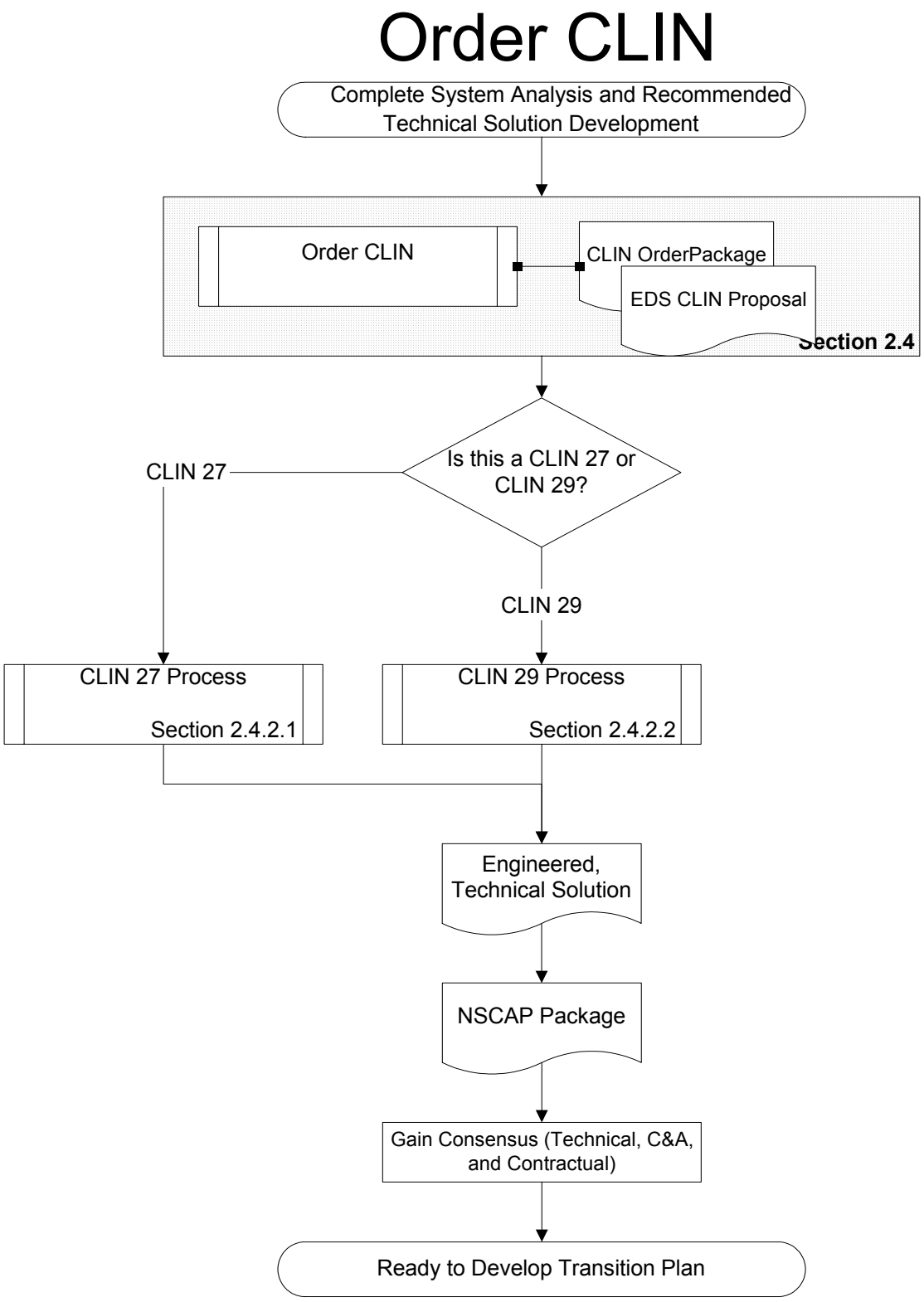


Figure 2-7 Order CLIN

2.5.1 CLIN Request Guidelines and Requirements

The CLIN Order is the mechanism that triggers initial integration services for operational and functional systems to enable them to transition to NMCI. In order for a Legacy System to be a candidate for CLIN 27, it must have the following characteristics: the client portion of the Legacy System has to be Windows 2000 compliant, all users must have NMCI seats, there can be no external server-initiated connection outside of NMCI to that Legacy System, and it has to have a completed the NSCAP. There are conditions where a CLIN 27 can be ordered for a server that makes a connection to a server outside of NMCI. These exceptions must be submitted and approved by the DAA prior to ordering a CLIN 27. For example: a portal server could connect to a "weather ticker" service through the NMCI DMZ.

CLIN 29 services provide a range of options that include, but are not limited to, EDS hosting of applications, operations and maintenance support, Service Level Agreement (SLA), database management, business process re-engineering, and training. Because of the flexibility of this CLIN, each CLIN 29 Order Package will be separately priced as individual orders with negotiated SLAs. However, as systems transition to the NMCI environment, EDS will create scenarios, which will be used as aids to expedite the ordering process (please refer to Appendix E: EDS CLIN Package Scenarios). A CLIN 29 order will be required for any Legacy System that requires a non-NMCI user access or other external connections that are not in accordance with DON security and IA policies as enforced in NMCI. Public access servers will need to be placed in a DMZ, which may incur a cost. The system will also be required to have completed the NSCAP.

2.5.2 Site Representative, CDA, and PM Complete CLIN Order Package

The submission of a CLIN Order Package is the first, formal process in transitioning any system to the NMCI environment. Consequently, all activities prior to completing the CLIN Order Package are directly in support of ordering the CLIN and subsequently transitioning the system to the NMCI environment. EDS Base Operations will serve as the local EDS representative for the CLIN Order process to ensure the CLIN Order Package is submitted according to specifications.

The Planning and Coordination Team and Site Representative, CDA, or PM identifies the requirements for the appropriate security groups, user rights and permissions in the CLIN Order Package. The Planning and Coordination Team and EDS Base Operations will work cooperatively to provide the EDS Business Office with all CLIN Order Package-supporting documentation (ST-ERQ, IATO/ATO, SSAA, etc).

Additionally, the CLIN Order Packages will identify the requirements for the seats needed to administer and manage the system. If these administration and management seats were not previously ordered, additional CLIN Order Packages will be required for the additional seats.

2.5.2.1 Process Requirements for CLIN 27

The Site Representative, CDA, and PM must complete the CLIN Order Package located at https://www.ecommerce.nmci-eds.com. Ordering CLIN 27 requires selection of bandwidth (L/M/H) and the determination whether mission critical option is necessary.

The Site Representative, CDA, and PM will be required to manage the system unless optional CLIN 29 for EDS management has been ordered. They are also required to identify and document provisions for future (e.g. hosting, sunset, etc.) desired services in conjunction with this option.

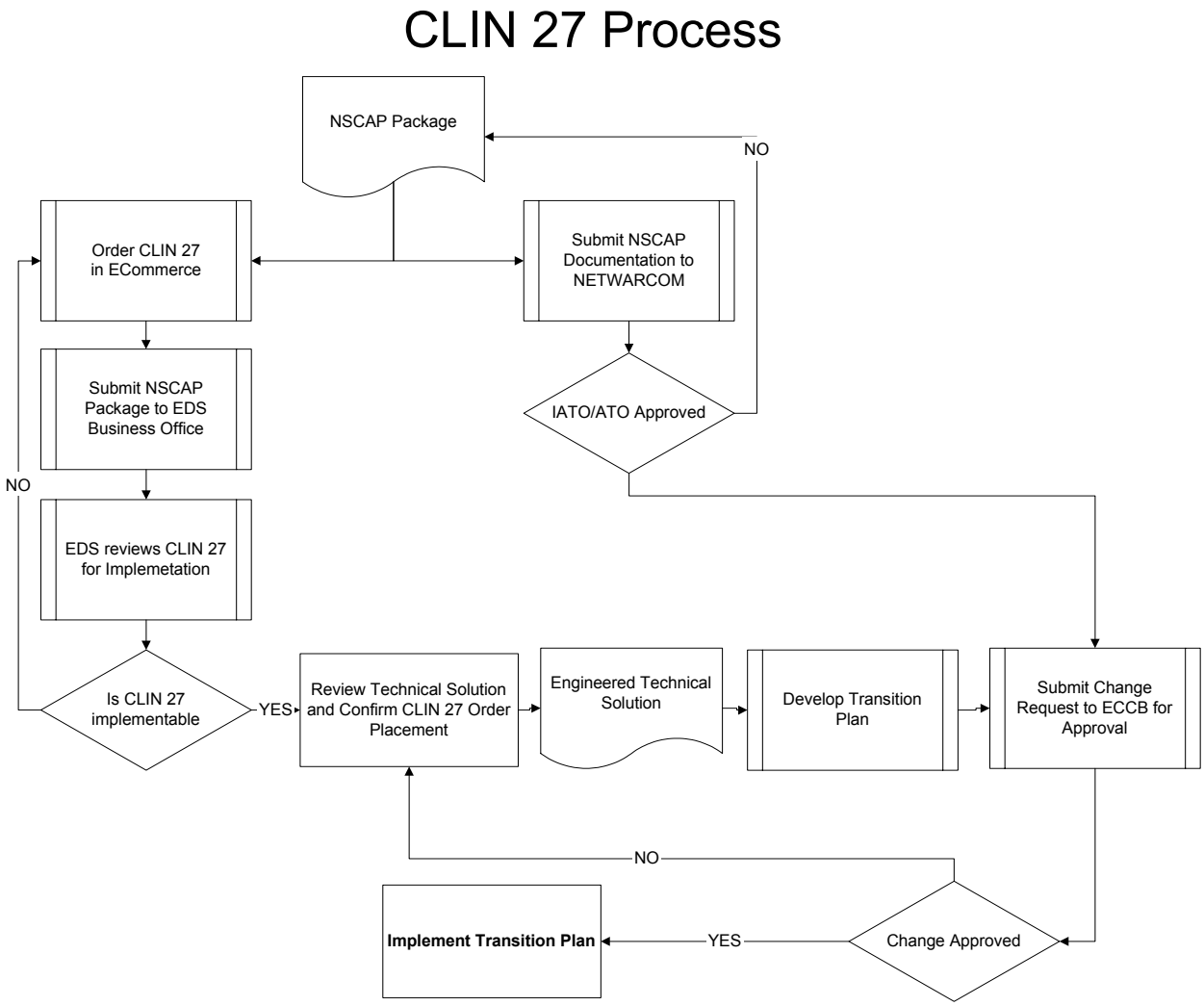


Figure 2-8 CLIN 27 Process

2.5.2.2 Process Requirements for CLIN 29

The Site Representative, CDA, and PM must complete the CLIN Order Package located at https://www.ecommerce.nmci-eds.com and the CLIN 29 questionnaire (please refer to Appendix D).

For the most current version of the questionnaire please refer to http://www.nmci-eds.com/CLIN29_Questionnaire.doc.

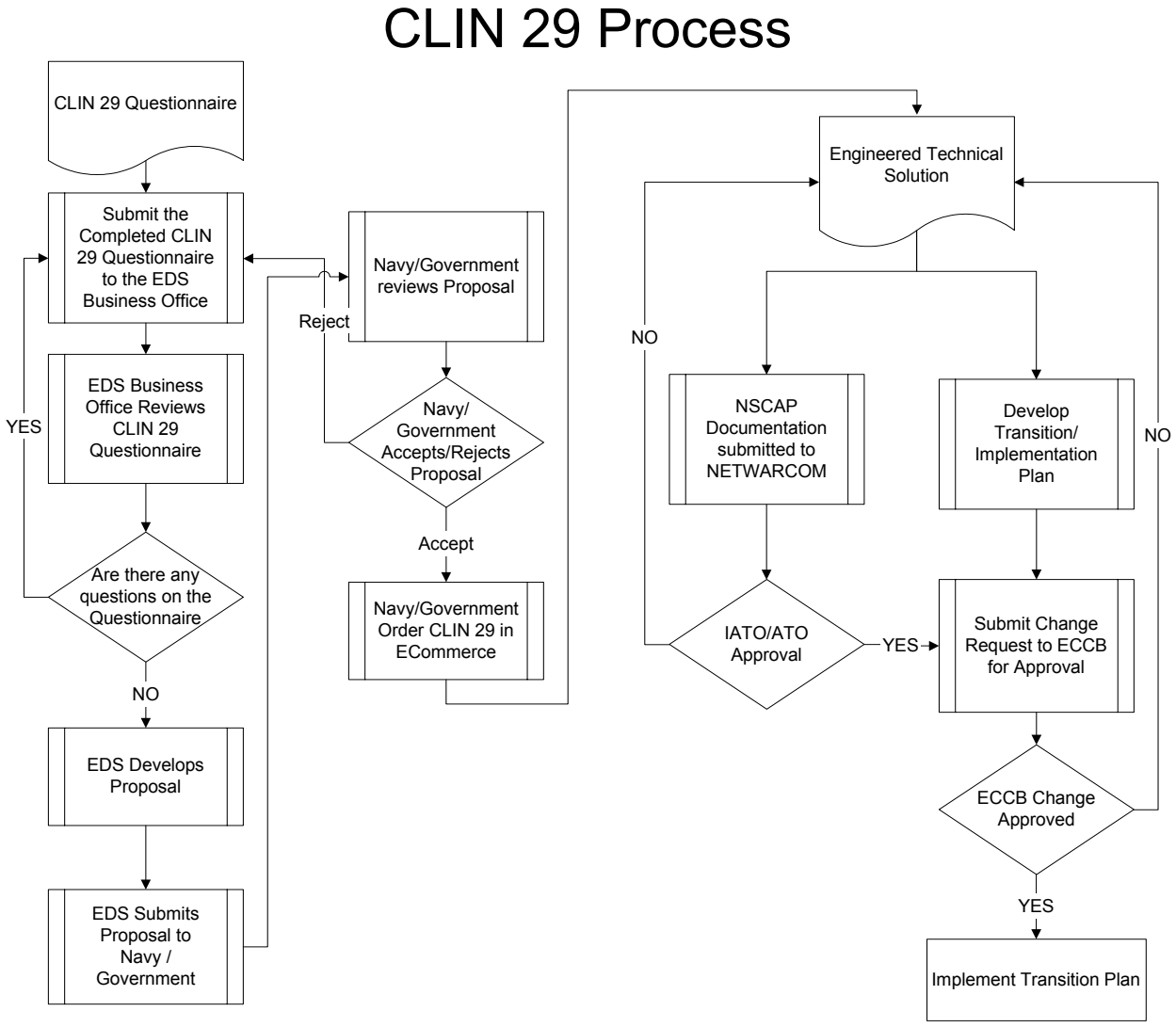


Figure 2-9 CLIN 29 Process

2.5.3 EDS Business Office Assesses CLIN Order Package and Submits Proposal

The EDS Business Office receives the CLIN Order Package and supporting documentation and acknowledges the receipt with a proposed date for a response to the CLIN Order Package.

2.5.3.1 EDS Business Office Assesses CLIN 27 Order Package

Upon completion of the processes, requirements and deliverables defined in this LSTG, the EDS Base Operations and/or NOC will implement and verify network connection. The Site Representative, CDA, and PM will validate the system operation. At that point, the EDS Business Office will initiate asset management, SLA reporting, and billing.

2.5.3.2 EDS Business Office Assesses CLIN 29 Order Package

The EDS Business Office will respond to the CLIN 29 order with a proposal to perform an assessment to identify the appropriate enterprise solution. The response time varies depending on the integration and

support services requested. Some "pre-packaged" responses can be done within a week; others may take much longer depending upon the complexity or the lack of similarity to CLIN 29 scenarios that have been identified through previous requests. In those cases, the estimated delivery time is within 2 weeks of receipt of the CLIN 29 request. Following the assessment, the EDS Business Office will submit a proposal to implement an enterprise solution based on the requirements identified in the CLIN 29 request. Upon Site Representative, CDA, and PM acceptance of this proposal and completion of the processes, requirements and deliverables defined in this LSTG, the EDS Base Operations and/or NOC will implement and verify network connection. The Site Representative, CDA, and PM will validate the system operation. At that point EDS will initiate asset management, SLA reporting, and billing.

2.5.4 Review Proposal and Accept Technical Solution

Upon receipt of the EDS proposal, the Site Representative, CDA, and PM will review the proposal, assess the complete Technical Solution, and review the assumptions for government-provided roles and resources. Additionally, the Site Representative, CDA, PM, and the Planning and Coordination Team will assess the total project to incorporate the total project schedule, resources, and costs as they apply to the total bottom-line cost to the government. The bottom-line cost includes the EDS proposal and any internal (non-EDS) costs to the government.

To assist the Site Representative, CDA, and PM in assessing the EDS proposal and the entire project, Risk Management Assessment Tools are included in Appendix H.

After assessing the Engineered Technical Solution, the Site Representative, CDA, and PM will accept or decline EDS' proposal. If the Site Representative, CDA, and PM decline the EDS proposal, the Site Representative, CDA, and PM may re-submit another CLIN Order Package to revise the requirements.

2.5.4.1 Document Government-Provided Roles & Resources Associated With the EDS Proposal

The Site Representative, CDA, and PM must identify and consider all of the required government roles and resources prior to accepting the EDS proposal. For a CLIN 27 the government will be required to provide all of the resources needed to manage and maintain the system. For a CLIN 29 proposal the required government resources will be determined by the EDS CLIN proposal and dependent on EDS providing the following services:

- Hosting
- Operations and maintenance support
- Database management
- Business process re-engineering
- Training

2.5.4.2 Assess the Complete Technical Solution, Incorporating Total Project Schedule and Cost

The Site Representative, CDA, and PM must also consider the total project schedule and costs prior to accepting the EDS proposal. As requested by the Site Representative, CDA, and PM, the IATT will advise in assessing the complete Technical Solution. For both a CLIN 27 and CLIN 29 proposal the Site Representative, CDA, and PM will need to ensure that the proposed schedule outlined in the EDS proposal will meet their expectations and will not jeopardize daily operations.

The Site Representative, CDA, and PM must also ensure they account for all costs above and beyond the EDS proposal before accepting the EDS solution. For a CLIN 27 proposal the Site Representative, CDA, and PM will be responsible for all of the costs associated with managing and maintaining the system after the transition and the selected CLIN 27 monthly fee. For a CLIN 29 proposal the additional costs will be determined by the services that will not be performed by EDS.

2.6 DEVELOP TRANSITION PLAN

The ECCB has final approval authority before proceeding into the Legacy System Transition Execution phase. The IATT in conjunction with the Site Representative, CDA, and PM, will manage the Develop Transition Plan phase of the System Transition as depicted in Figure 2-10. The objective of this phase, depicted in Figure 2-10, is to develop the Transition POA&M, prepare the NMCI environment for the System Transition, prepare and submit the NSCAP Package, and prepare the Legacy System and its Supporting and Interfacing Systems for transition into NMCI. To capitalize on the knowledge and experience associated with the Engineered Technical Solution, the IATT will support the development of the System Transition Plan, which includes the Transition POA&M, SOVT, Test Plans, and any additional documentation. Additionally, the IATT will provide C&A guidance necessary for development of the Transition Plan.

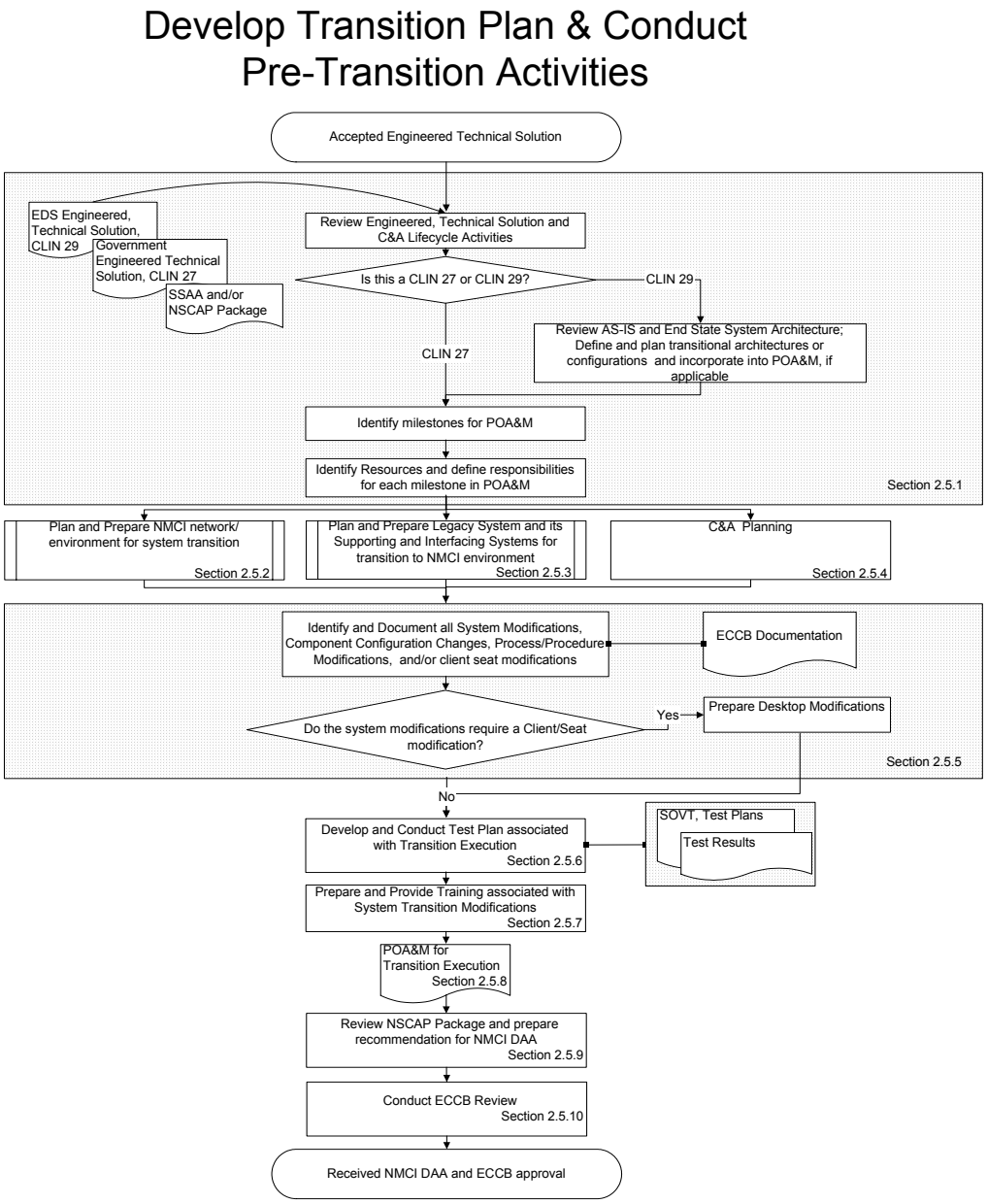


Figure 2-10 Develop Transition Plan & Conduct Pre-Transition Activities

2.6.1 Review Engineered Technical Solution and C&A Life Cycle Activities

The Site Representative, CDA, PM, and the Site C&A Team will complete the NSCAP Package for each system transitioning to the NMCI environment. Please refer to http://www.infosec.navy.mil for the current NSCAP specification. Under the direction of the Certification Authority, the IATT will assist the Site in review of the completed NSCAP Package prior to submission to the NMCI Connection Approval Review Panel (NCARP). The Team Leader will deliver the NSCAP Package to the NCARP, which reviews the NSCAP Package and submits a recommendation to the Navy NMCI DAA for approval.

The IATT, Site Representative, CDA, and PM must review the Engineered Technical Solution and the C&A Life Cycle activities including the NSCAP Package to complete the Transition POA&M. The

Transition POA&M should outline each milestone for the initial transition and end state architecture, and identify the specific team and/or individual responsible for each milestone.

2.6.2 Plan and Prepare NMCI Network/Environment for System Transition

The IATT, Site Representative, CDA, and PM must ensure the NMCI Network/Environment is prepared for the System Transition as depicted in Figure 2-11. Transitioning servers will potentially have conflicting host names; therefore, each Site Representative, CDA, and PM must contact the EDS Base Operations, NOC and NMCI Help Desk to register their host name and in some cases request a new host name. Only IP addresses in the DMZ are routable IPs. Systems in the Trusted Enclave will receive private non-routable IP addresses. Integration into the NMCI Active Directory Services is desired for all Microsoft Windows 2000 compliant systems. These activities should include the following:

- Identify resources and define responsibilities for each milestone in the Transition POA&M.
- Develop Backout/Rollback procedures for NMCI environment.
- Engineer any boundary considerations/architectural placement issues.
- Incorporate existing maintenance schedule.
- Request/Receive NMCI Local Area Network (LAN) connection.
- Request/Receive static IP and NMCI compliant names.
  - NMCI Host Name (Fully Qualified)
  - NMCI IP Address and subnet mask
  - NMCI Default Gateway IP Address
  - NMCI DNS Server Address
  - NMCI WINS Server Address
  - NMCI Active Directory
- Submit request to NMCI to plan for environment changes.

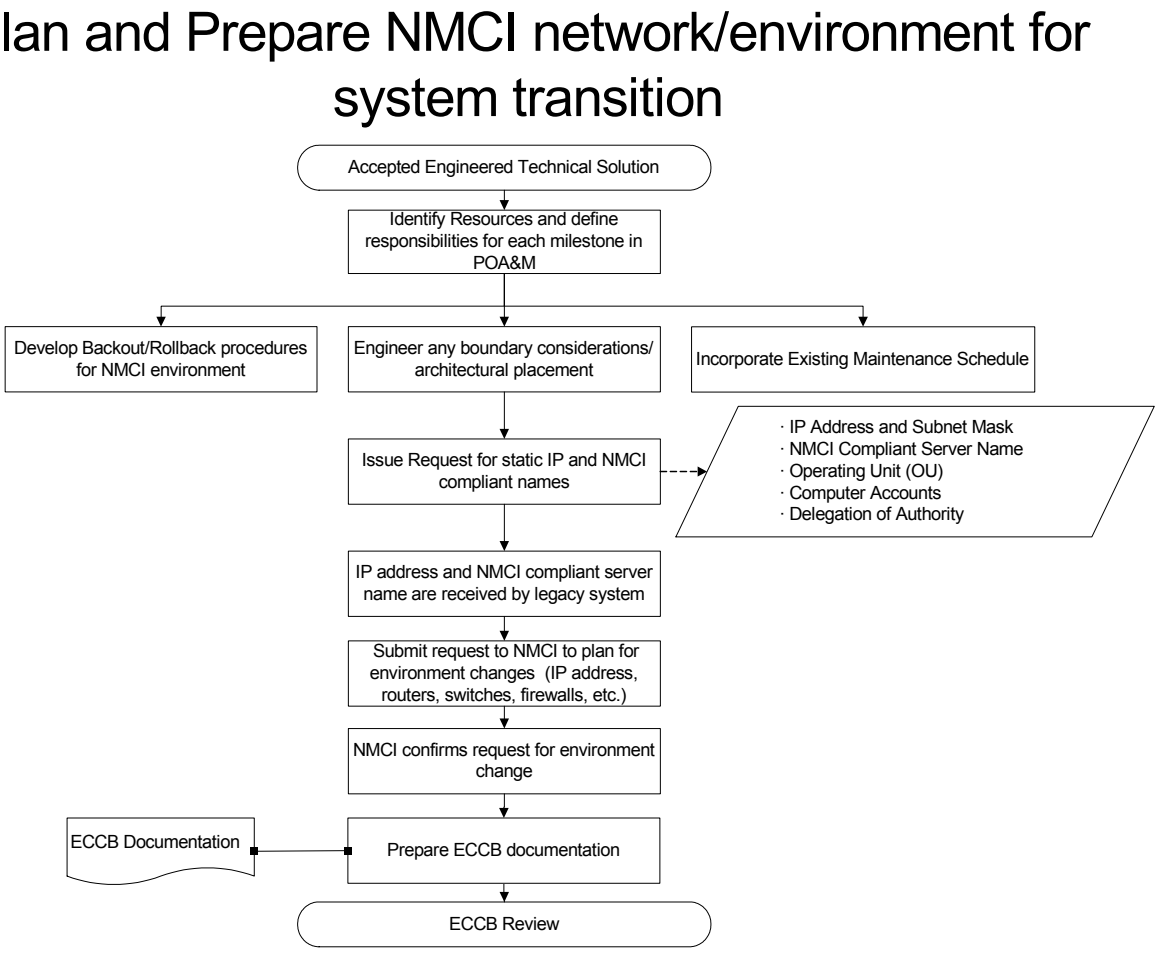


Figure 2-11 Plan and Prepare NMCI network/environment for system transition

To facilitate an efficient transition execution, the Implementation Team will assist in the planning and preparation of the NMCI network environment.

2.6.3 Plan and Prepare Legacy System and its Supporting and Interfacing Systems for Transition to NMCI Environment

The IATT, Site Representative, CDA, and PM must ensure the Legacy System and its Supporting and Interfacing Systems are prepared to transition into the NMCI Network/Environment as depicted in Figure 2-12. To facilitate efficient transition execution, the Implementation Team will assist in the planning and preparation of the Legacy System and its Supporting and Interfacing Systems. The IATT, Site Representative, CDA, and PM must identify the existing maintenance schedule for the Legacy System and its Supporting and Interfacing Systems, develop Go/No-Go criteria, and prepare backout and rollback procedures that will be included in the System Transition Plan.

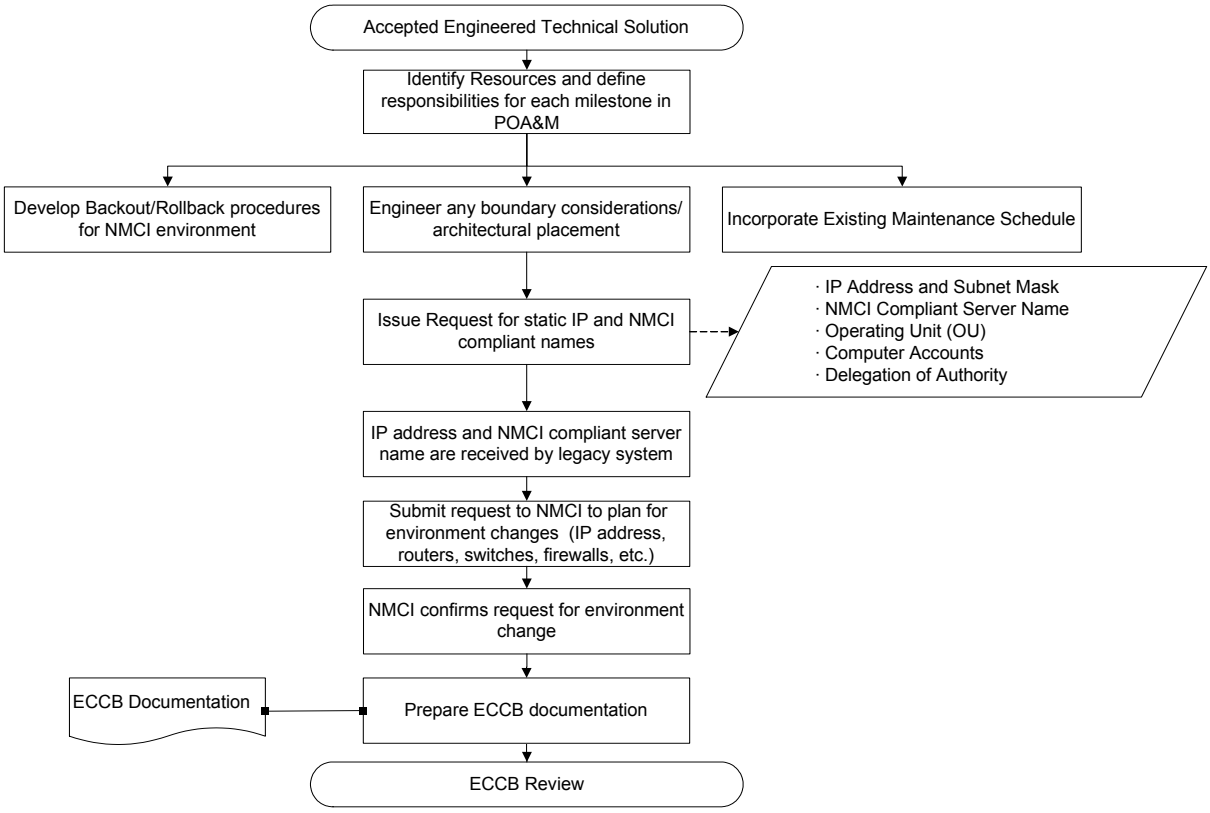


Figure 2-12 Plan and Prepare Legacy System and its Supporting and Interfacing Systems for transition to NMCI environment

Additionally, while preparing the Legacy System and its Supporting and Interfacing Systems for transition, the Planning and Coordination Team, EDS Base Operations, Site Representative, CDA, and PM should complete the following:

- Identify resources and define responsibilities for each milestone in the Transition POA&M.
- Incorporate existing maintenance schedule for Legacy System and Supporting and Interfacing systems.
- Work with Site Representative, CDA, and PM to define Go/No-Go criteria and rollback criteria that are unique to the system transitioning.
- Prepare the backout and rollback plans for the Legacy System, supporting systems, and interfacing systems.
- Review and update architecture diagrams and identify any hardware modifications or upgrades (provide updates as applicable to NMCI Help Desk or NOC for procedural modifications).
  - COTS vendor package upgrades/patches/fixes (capturing vendor recommendation and vendor case #).
  - Utility upgrades—backup/restore software, configuration management software, system monitoring utility tools, etc.

  - Custom application build version – documenting any unique configuration items associated with the build (database modifications, supporting wrapper scripts, supporting custom utilities, etc.).
  - OS or COTS/vendor configuration modifications (kernel changes, compilation issues or settings, version compatibility requirements, etc.).
  - Network/security modifications (pending CERT advisories, IP addresses, subnet masks, tripwire, firewall, access lists, etc.) typically stored/documented on another server or trusted system or printed and stored in a secure location.
- Prepare NMCI Help Desk support for anticipated outage associated with System Transition.
- Initiate any government work orders for facilities or other non-EDS or non-NMCI requirements.
- Submit EDS Work Request.
- Refine Transition POA&M with results from planning and preparation activities.

2.6.4 C&A Planning

A C&A POA&M for follow-on risk mitigation activity is required by the Navy NMCI DAA for Legacy Systems/applications being considered for transition to the NMCI environment. Many such Legacy Systems/applications were not fielded with all necessary evaluation and documentation. The NSCAP provides guidance to Site Representative, CDA, PM, and system/application owners to determine the appropriate level of effort necessary to ensure a valid, accurate assessment of risk. The assessment of risk will then be used by the Navy NMCI DAA when considering approval to transition the system/application to NMCI. Section 4.4 of the NSCAP provides greater detail of the comprehensive C&A POA&M, which contains a Vulnerability Assessment and a Risk Analysis. Sections 4.1, 4.2 and 4.3 of the NSCAP provide detailed information regarding C&A Planning.

- Execute C&A Planning
  - Review the C&A POA&M, identify all required resources, and define responsibilities.
  - Identify all remote user locations for testing.
  - Determine activities for hardening and ST&E testing.
  - Identify communication plan to inform all users that system will be down for testing.

- Perform hardening activities in preparation for System Transition
  - Perform pre-hardening Vulnerability Scan of system.
  - Review results of the pre-hardening Vulnerability Scan of system and propose hardening changes.
  - Analyze proposed hardening changes to other applications residing on the server or interfacing systems.
  - Harden OS (each server).
  - Harden application (install updates & security patches to include Information Assurance Vulnerability Alert (IAVA) and Information Assurance Vulnerability Bulletin (IAVB)).
  - NMCI Security Augment (h.scripts, A-V, host IDs, and Enterprise Management System (EMS) Conf.).
  - Test application for functionality and typical operations (back ups, security rules are intact, system administration functions, etc.).

Hardening activities ensure systems/applications meet the minimum IA requirements of the NMCI enclave. Sections 5 and 6 of the NSCAP provide detailed information regarding the incorporation of

hardening activity results into the NSCAP Package. Additionally, Section 4.3 of the NSCAP contains a list of the minimum NMCI IA requirements.

EDS will likely want to run "hardening scripts" to host servers within NMCI. This is to ensure the legacy server risk to NMCI is reduced.

2.6.5 Identify and Document all System Modifications, Component Configuration Changes, Process/Procedure Modifications, and/or Client Seat Modifications

Once the NMCI environment, Legacy System, and its Supporting and Interfacing Systems are prepared for transition, the IATT, Site Representative, CDA, and PM must submit a Release Deployment Plan outlining all system modifications, component configuration changes, process and procedure modifications, and client/seat modifications (refer to the NRDDG or Legacy Application Transition Guide (LATG) for client/seat modification procedures) to the Enterprise Change Control Board (ECCB) for approval.

The IATT, Site Representative, CDA, and PM will be responsible for ensuring all non-software changes are properly documented in their respective documents (Standard Operating Procedures (SOPs), procedures, network or architecture diagrams, etc.) and properly prepared for implementation in both production and supporting systems.

As systems transition into NMCI, there may be instances when software must be modified to support both NMCI and Department of the Navy requirements. In many cases, these modifications must be applied to the system and/or supporting desktop software (either a configuration or software change). These changes will require the desktop software to follow a pre-defined release management process. The release management process is a coordinated effort between the CDA and EDS and should be accounted for in the Transition POA&M. For information on the release management process, please refer to the NRDDG and the LATG http://www.nmci-eds.com/legacy_applications_transition_guide.pdf.

Throughout the entire System Transition Process, changes, modifications, or enhancements in the production and support systems may be recommended. These recommendations will be reviewed and/or approved by the IATT, Site Representative, CDA, and PM prior to inclusion in the System Transition plan.

2.6.6 Develop and Conduct Test Plan associated with Transition Execution

The IATT, Site Representative, CDA, and PM should also develop pre- and post- Test Plans, update the SOVT, set up the test environment, and assign technical staff to execute testing. In addition to ensuring that the system can accomplish its core mission in the NMCI environment, the Test Plans will include specific testing associated with any system changes, modifications, or enhancements.

The Test Plan will include input from the System Assessment and its associated ST-ERQ. The goal of the Test Plan is to document the tests associated with system changes as related to the transition. Therefore, the Test Plan will clearly address the following functional, technical and security tests:

- Describe the test environment (including hardware, operating system, tools, utilities, printing, applications, scripts/wrappers, network configuration, etc.).
- Clearly define the differences between the test environment and the production environment to mitigate any risks in transition execution (simulators, network differences, smaller database, hardware configuration, any application or COTS version/patch discrepancies, etc.).
- Document any assumptions associated with the environment or data used during testing.

- Define real data requirements and/or simulated data requirements per test scenario/case.
- Incorporate subject matter experts in Test Plan/procedure development and test execution.
- Categorize the types of testing expected to perform: system (integration) or software (unit/string).
- Cross-reference every system change/modification to some form of test (integration or unit/string).
- Publish a proposed schedule for test execution.
- Work with Site Representative, CDA, and PM to define exit criteria and update Go/No-Go criteria and rollback criteria as related to the candidate system.
- Work with Systems Coordinator and Software Coordinator to develop tests for rollback or back out approach.

The IATT, Site Representative, CDA, and PM develop the templates associated with test scenarios/cases that capture the results for each test (records based, transaction based, etc.). A simple example is depicted below:

- Obtain existing system documents/test cases.
- Develop procedures to test component and overall functionality.
  - Component functionality test.
    - Hardware, Network, and Application specific.
- Develop ST&E Plans & Procedures.
  - Site Representative, CDA, and PM review and approve Plans & Procedures.
- Test overall functionality of System using SOVT.
  - Site Representative, CDA, and PM review & approve SOVT.

Using the Test Plan, preliminary testing in support of transition planning will be conducted to minimize risk associated with the Legacy System transitioning to the NMCI environment. Therefore, the preliminary testing will include the following functional, technical, and security tests:

- Capture any test environment anomalies (including hardware, operating system, tools, utilities, applications, scripts/wrappers, network configuration, etc.).
- Confirm any documented or newly identified differences between the test environment and the production environment to mitigate any risks in transition execution (simulators, network differences, smaller database, hardware configuration, any application or COTS version/patch discrepancies, etc.).

2.6.6.1 Report Test Results

Integration testing is the primary form of testing. It is assumed all unit or string testing associated with software or legacy application changes will be completed prior to executing system tests. If possible, the entire cutover process (execution) and rollback/back out process should be tested in sequence.

During the execution of system tests, the Planning and Coordination Team confirms the assumptions annotated in the Test Plan and ensures the technical staff follows the test execution scenarios and populates the test execution templates with actual results.

Additionally, reporting of test results should document any additional information associated with the testing, and should include:

- Assumptions associated with the environment or data used during testing.
- Discrepancies with real or simulated data per test scenario/case.
- Input for Go/No-Go criteria and rollback criteria.
- Configuration items or system modifications required to successfully transition the system.

2.6.6.2 Recommend Corrective Action, Revise Schedule, and/or Transition POA&M

The Transition Plan is developed from the entire team's input compiled and refined as the result of the preparation and testing activities. The development of the Transition Plan is an iterative process that requires regular monitoring and updating. If applicable, the technical staff will provide revisions to the schedule or Transition POA&M to incorporate test results.

Sample recommended corrective actions include:

- Updates to system rollback or back out procedures.
- Recommendations to acquire missing resources (labor, equipment, licenses/software, maintenance agreement modifications).

2.6.7 Prepare and Provide Training associated with System Transition Modifications

The Planning and Coordination Team, Site Representative, CDA, and PM should prepare and provide training to all concerned parties (e.g. system users, system administrators, NOC, etc.) on the modifications of the system and the transition execution, and complete the Transition POA&M for the Legacy System Transition Execution phase.

2.6.8 Plan of Action and Milestones (POA&M) for Transition Execution

The POA&M allows the Site Representative, CDA, PM, and the Planning and Coordination Team to plan the System Transition in a detailed fashion with dependencies and resources annotated. With support from the Planning and Coordination and Implementation Teams, the Site Representative, CDA, and PM are responsible for completing the Transition POA&M. The EDS Base Operations will provide guidance to ensure EDS responsibilities (EDS Base Operations, NMCI Help Desk, and NOC) are identified in the Transition POA&M and that the Transition POA&M adheres to the accepted CLIN proposal. Please refer to Appendix G for a sample Transition POA&M.

2.6.9 Review NSCAP Package and Prepare Recommendation for Navy NMCI DAA

The NSCAP Package review will be conducted by the NCARP, which consists of the following voting representatives: Navy NMCI DAA, PMW 161, the USMC DAA, the PMO, and a non-voting EDS representative. The Site Representative, CDA, and PM present the NSCAP Package. At the conclusion of the NSCAP Package review, the NCARP prepares a recommendation for the Navy NMCI DAA.

2.6.10 Conduct ECCB Review

The Enterprise Change Control Board provides joint Government and EDS oversight of changes to the NMCI environment and ensures that decisions are based upon situational awareness of ongoing military operations. The ECCB is comprised of representative management from each EDS Functional area including Enterprise Architecture, Systems Engineering, Enterprise Engineering, Proving Center Lab, Solution Certification, Enterprise Operations, Site Transition, Field Services, as well as customer representation from the Navy Operations, Navy Security, USMC Operations, USMC Security and the DON Major Claimant (MC) PMO. The ECCB meets on a regular basis in reviewing change requests.

2.7 EXECUTE SYSTEM TRANSITION

The objective of the System Transition Execution phase, depicted in Figure 2-13, is to successfully transition the Legacy System and its supporting/interfacing systems to the NMCI environment. With significant planning, coordination, preparation, and technical engineering prior to this phase, transitioning the Legacy System to the NMCI environment should simply be a detailed, coordinated execution of the Transition Plan. The Legacy System Transition Execution process depicts the simple process of transition execution with intermediate checkpoints to determine success as mapped to the Transition Plan.

Prior to executing the System Transition, the system must have Navy NMCI DAA approval and ECCB notification.

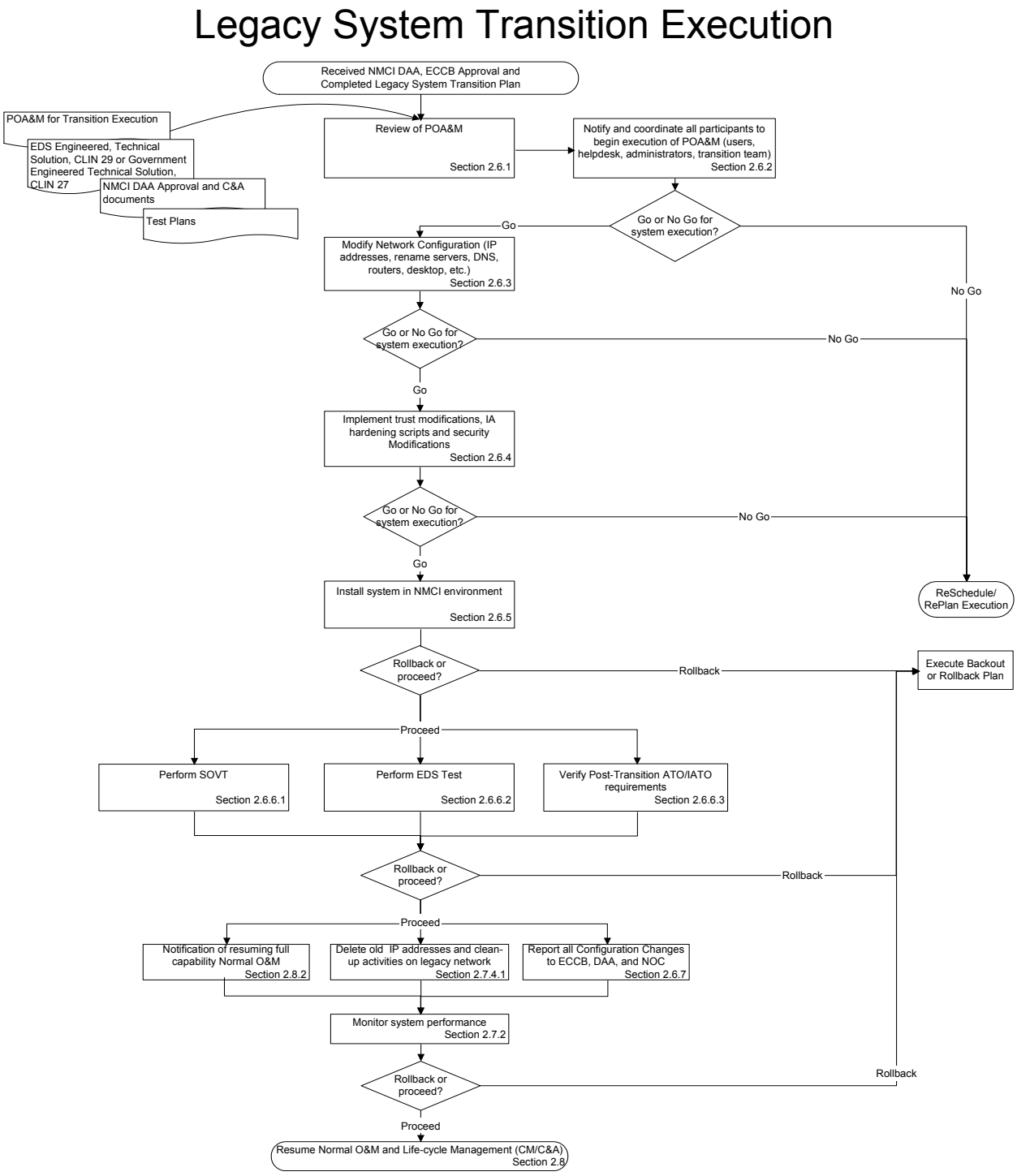


Figure 2-13 Legacy System Transition Execution

2.7.1 Review of Transition POA&M and Test Plan

Prior to the scheduled Legacy System Transition Execution period, the Planning and Coordination Team provides to all participants and interested parties the Transition POA&M. If applicable, the participants will receive copies of SSAA, NSCAP Package, or Test Plan.

The Planning and Coordination Team leads the final review of the Transition POA&M and Test Plan with all participants. For more complex executions, the Planning and Coordination Team may establish a "virtual command center" for centralized coordination and communication. The "virtual command center" may be an ongoing conference call, an electronic notification process, or an internal website, which all facilitate quick notification of status and team communication. The goals during the final review of the Transition POA&M include:

1. Highlighting the schedule.
2. Confirming that any prerequisite preparations (hardware, software, license or maintenance activities) are complete.
3. Confirming each participant's responsibilities and contact information.
4. Confirming the dependent and parallel activities.
5. Reinforcing the Go/No-Go and Rollback criteria.
6. Reviewing the criteria for resuming normal operations and maintenance.
7. Reviewing the Test Plan prerequisites in the context of the Transition POA&M.

2.7.2 Notify and Coordinate all Participants to Begin Execution of Transition POA&M

After completing the final review of the Transition POA&M and Test Plan with all participants, the Planning and Coordination Team notifies the Implementation Team to begin the execution of the Transition POA&M. The Planning and Coordination Team has the responsibilities of monitoring the schedule and facilitating communicating status across the team. The NMCI Help Desk will handle all help desk calls during the System Transition and will provide users a current status of System Transition.

Additionally, the Planning and Coordination Team will notify all users of the scheduled activity using the communication process typical to this type of maintenance activity. An example includes a broadcast message indicating the system will be unavailable, specifying the estimated period of unavailability or limited capability. The following organizations or entities should be notified or included in any broadcast communications:

1. EDS Base Operations and NOC
2. All Users
3. Interfacing Systems' POC
4. NMCI Help Desk and other Help Desks (if applicable)
5. Legacy System Transition Team participants
6. C&A Personnel
7. Change Management and Quality Assurance (CM and QA)

2.7.3 Modify Network Configuration

All systems transitioning to the NMCI environment will require some form of network modification. Also, each system transitioning to NMCI will require the EDS Base Operations and NOC to take action to accomplish the network modification.

As outlined in the Transition POA&M, all system devices requiring configuration changes will need to be modified. System devices include servers, switches, routers, firewalls, Channel Service Units/Digital Service Units (CSU/DSU), printers, tape drives, storage libraries, etc.

2.7.4 Implement Trust Modifications, IA Hardening Scripts, and Security Modifications

The Site C&A Team, in conjunction with the Implementation Team, will perform hardening activities as outlined in the Transition POA&M and any NSCAP requirements.

- Harden OS (ea server).
- Harden application (install updates & security patches).
- NMCI Security Augment (h.scripts, A-V, host IDS, and EMS Conf.).
- Perform post-hardening Vulnerability Scan of system.

2.7.5 Install System in NMCI Environment

Under direction of the Planning and Coordination Team, all participants will actively follow the Transition POA&M and any detailed associated procedures to successfully transition the Legacy System to the NMCI environment.

2.7.6 Testing

Following the installation, the Test Plans defined during the Transition Planning phase will need to be conducted to test for NMCI compliance, IA vulnerabilities, and specific testing criteria based on the accepted CLIN proposal. The Planning and Coordination Team, Site Representative, CDA, and PM will need to ensure the they notify the DoD/DON and all concerned parties that the system will encounter limited service interruptions during testing.

2.7.6.1 Perform System Operational Verification Test (SOVT)

A SOVT will be completed and signed by the appropriate signatory to verify that the system is performing operation functions in the NMCI environment. Refined during the Transition Plan, the SOVT gives CDA or PM the opportunity to specifically test their system operational capability in the NMCI environment.

Ideally, similar quantifiable test results obtained by performing a SOVT in the legacy environment will be compared against the test results obtained by performing the SOVT in the NMCI environment.

2.7.6.2 Perform EDS Test

The EDS Base Operations and NOC will ensure that a testing process will be developed that will support the appropriate CLIN Order. Depending upon the requirements of that CLIN Order, EDS Base Operations and NOC will perform the appropriate testing and participate in the SOVT.

2.7.6.3 Verify Post-Transition IATO/ATO Requirements

Under the direction of the Navy NMCI DAA, the Site C&A Team will conduct security testing to verify that the post-transition IATO/ATO requirements have been met. During post-Execution Activities, the Site C&A Team will re-verify IATO/ATO requirements and report findings to the Navy NMCI DAA.

2.7.7 Report all Configuration Changes to ECCB, DAA, and NOC

The NOC will serve as a participant during the Legacy System Transition Process. After successfully transitioning the system to the NMCI environment, the Planning and Coordination Team will compile all changes/modifications as part of the System Transition and provide the compiled list to the NOC, ECCB, and DAA.

Equipped with a compiled list of planned changes/modifications, the NOC can proactively monitor the network for performance, bandwidth utilization, and, if applicable, monitor hardware performance.

2.7.8 Execute Backout or Rollback Plan

As a result of Transition Plan, each system will have developed backout or rollback checkpoint criteria. One type of rollback checkpoint criterion is determining if the system should be backed out of the NMCI environment and return to the legacy environment. If the checkpoint criteria are not met, the Site Representative, CDA and PM will initiate the backout or rollback plan with guidance from the Planning and Coordination Team and EDS Base Operations.

2.7.9 ReSchedule or RePlan Execution

One type of checkpoint is determining if the System Transition should be rescheduled or replanned. Developed with the Transition Plan, each system will have developed criteria for the reschedule or replan checkpoint. Natural disasters, e.g. hurricane, could be a criterion to reschedule the System Transition. If the checkpoint criteria are not met, the Site Representative, CDA and PM will reschedule the System Transition with guidance from the Planning and Coordination Team and EDS Base Operations.

2.8 CONDUCT POST-EXECUTION ACTIVITIES

The Post-Execution Activities will be managed by the Planning and Coordination Team, with support from the Implementation Team, the Site Representative, CDA, and PM. The objectives of these activities are to ensure that the system will be able to successfully resume normal operations and maintenance. This phase of the System Transition will include verifying that the post-transition IATO/ATO requirements are met, that the post-transition testing and monitoring criteria are satisfied, that the legacy network is decommissioned, and that the SOVT is signed.

2.8.1 Verify Post-Transition IATO/ATO Requirements

The Navy NMCI DAA is responsible for verifying that all of the post-transition IATO/ATO requirements have been met. The Navy NMCI DAA may designate the Site C&A Team, EDS, or Certification Agent to conduct the testing.

2.8.2 Monitor System Performance

After transitioning the system to the NMCI environment, the system should be monitored by EDS and the server hosting activity. As determined during the development of the Transition Plan, the monitoring period should include at least one full day of business/transactions and one full cycle of maintenance.

To facilitate comprehensive monitoring, users should be encouraged to perform one complete cycle of typical daily business activities, to include use of VRUs, printers, fax servers, scanners, digital displays, or Text Telephone (TTY) equipment within the established period defined during the Transition Plan. Critical maintenance activities, such as backups, should be monitored very closely during the first complete backup cycle of the system.

2.8.3 Access Controls

The Implementation Team will be responsible for configuring and implementing the security group policies and the user rights and permissions outlined in the accepted CLIN proposal.

2.8.4 Legacy Network Clean-up Activities

Once it is confirmed that the post-transition IATO/ATO requirements are met, the post-transition testing and monitoring criteria are satisfied, and the SOVT is signed, the Planning and Coordination Team, Site Representative, CDA, and PM will need to ensure that the legacy network is decommissioned. This process should include deleting the old IP addresses, terminating any legacy trusts, and disconnecting the legacy LAN connections.

2.8.4.1 Delete old IP Addresses

Security breaches are often a result of exploiting old IP addresses, unused IP addresses, old accounts, or easily guessed passwords. Either from within or external to the network, these security risks can be mitigated by deleting old IP addresses, removing old IP addresses from access lists or configuration files (removing legacy DNS entries), removing static routes, verifying all firewalls, routers, and switches have been properly cleaned up or re-configured, and spot checking any workstation/client configuration file modifications.

2.8.4.2 Terminate Trusts

In many cases, System Transition will itself resolve application transition issues, because certain applications were quarantined during the Rapid Certification Phase (RCP)/cutover due to B2 (Boundary 2) failures (i.e., inability of a client application located on an NMCI seat to communicate successfully with a quarantined/unmigrated server). Also, in many cases, domain trust relationships have been created to support communications between users who have been migrated to NMCI and the Legacy System. Once the system is established on the NMCI network, these trusts will no longer apply, and a request to the NOC shall be made by the Site Representative to remove ("break") them.

2.8.4.3 Disconnect Legacy LAN Connections

Once the system has successfully transitioned to the NMCI environment and successfully completed all the testing and IATO/ATO requirements, the Site Representative, CDA, and PM should disconnect all of the Legacy LAN connections.

2.9 RESUME NORMAL OPERATIONS AND MAINTENANCE & LIFE CYCLE MANAGEMENT

2.9.1 Service Level Agreements Resume

Each CLIN 27 has pre-established service levels for the network connection provided. CLIN 29 SLAs will be initiated when the system resumes normal operations and maintenance.

2.9.2 Notification of Resuming Full Capability Normal O&M

All users should be notified when the system resumes full capability. Providing a reminder or update on the system modifications (as they apply to the users) will reduce trouble calls and increase awareness. Additionally, all users should be notified of the scheduled activity using the communication process typical to this type of maintenance activity.

2.9.3 Augmented Staff Departs

During the System Transition, additional or augmented staff may support the transition. After the system resumes normal operations and maintenance, the Implementation Team and any additional or augmented staff will depart. The Planning and Coordination Team will conduct a formal hand-off to the O&M staff.

2.9.4 Resume the Normal Life Cycle Process of Change Control: ECCB, DAA, and NOC

With the system resuming normal operations and maintenance activities, the normal change control processes will also resume. Typically, an ECCB will review and approve changes for a system or the entire enterprise. Given the recently transitioned system's residence in the NMCI environment, the NMCI ECCB participants will assume their respective roles on the ECCB. Specifically, the Navy NMCI DAA and the NOC representatives will participate in reviewing changes as they apply to their respective areas, security and NMCI environment.

2.9.5 Continue C&A POA&M Activities associated with Post-Transition

The Site C&A Team under the direction of the Navy NMCI DAA will continue C&A POA&M activities associated with post-Transition.

- Satisfy any IATO/ATO conditions or directives placed on the system from Navy NMCI DAA, Developmental DAA, or other higher authorities
- Continue with re-accreditation activities associated with normal C&A lifecycle activities (upgrades, modifications, re-accreditation decisions).
- Update C&A documentation.

2.9.6 Operations and Maintenance Processes and Procedures Resume

For each CLIN 27 Order, the Site will resume its normal operations and maintenance duties. For each CLIN 29 Order, the operations and maintenance duties will be determined as part of the negotiated, accepted CLIN 29 proposal. The CLIN 29 EDS-provided services may range from only network support to full assumption of all operations and maintenance duties associated with the system. The EDS Base Operations and/or NOC will assume any responsibilities outlined in the requirements of the accepted CLIN proposal. Additionally, the EDS Base Operations and NOC will develop and implement new processes or procedures based on the system modifications associated with the requirements annotated in the accepted CLIN proposal.

2.9.6.1 EDS Help Desk Notification

The NMCI Help Desk will assume help desk roles as defined in the accepted CLIN proposal.

Whenever there is a planned system outage, the NMCI Help Desk is to be notified of that outage. If the outage is planned at a Site Operations level, then the individual that is planning for the system outage is to notify the Site Manager of the anticipated outage. The Site Manager will then take the appropriate steps to ensure that the NMCI Help Desk is properly notified. For the Help Desk notification procedures please refer to http://www.nmci-eds.com/helpdesk.htm.

If the outage is planned at an enterprise level, then the individual that is planning for the system outage is to notify the appropriate NOC Manager. The NOC Manager will then take the appropriate steps to ensure that the NMCI Help Desk is properly notified.

3.0 C&A ACTIVITIES

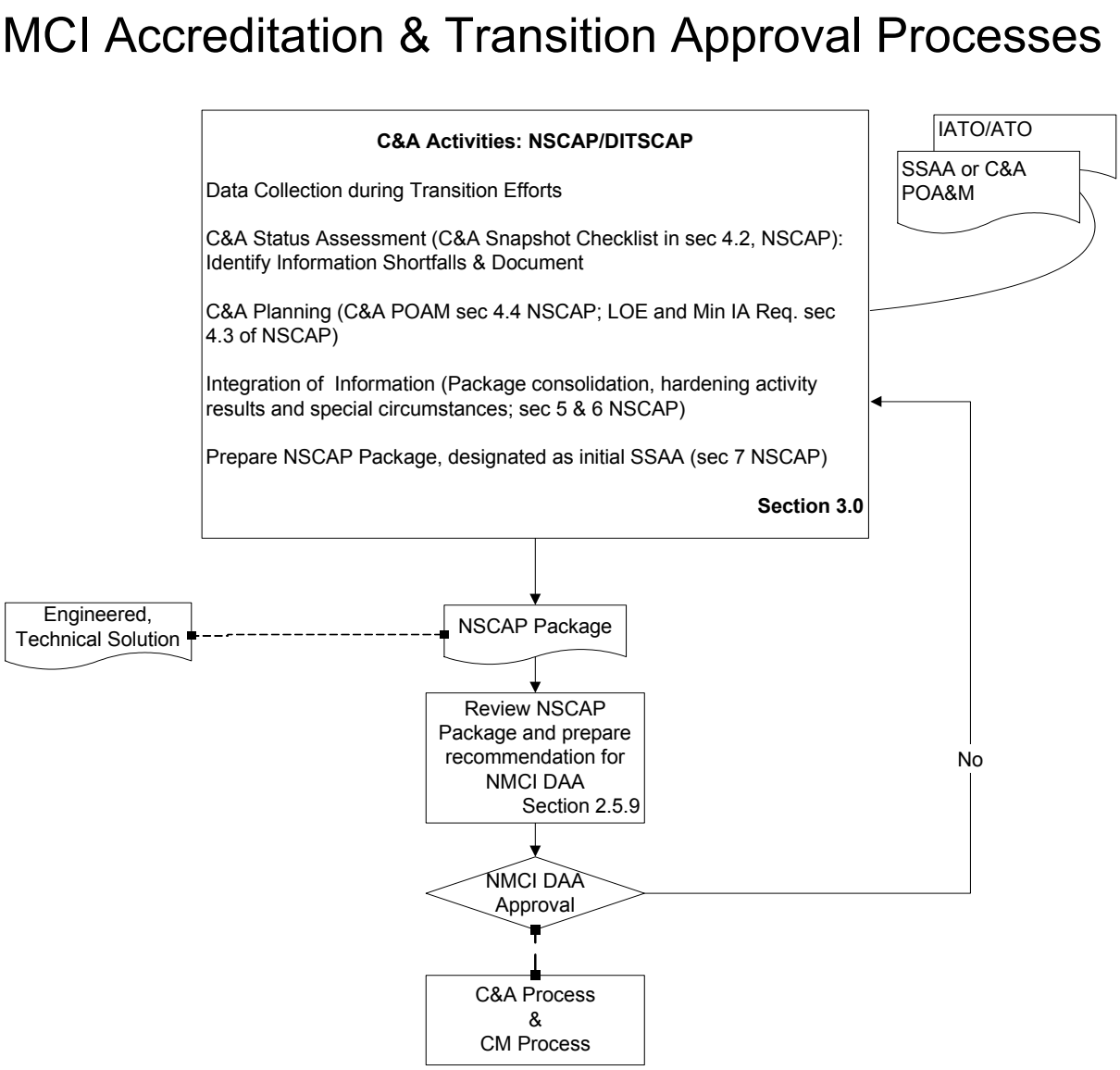


Figure 3-1 NMCI Accreditation & Transition Approval Processes

All systems wishing to transition to NMCI must meet DoD and DON security certification and accreditation criteria, and will therefore be evaluated by the NSCAP. The NSCAP will assist in understanding a candidate Legacy System's current C&A status. This is an essential requirement prior to proceeding with any extensive transition planning efforts. If a candidate Legacy System does not have a complete accreditation package, the NSCAP will guide the Site Representative, CDA, and PM to attain accreditation and IATO or ATO prior to executing the system transition, and will define the required material to prepare and present to the Navy NMCI DAA for transition approval.

Accreditation in the DoD requires that all Information Systems processing, handling, transmitting, or storing DoD information enable all appropriate protection measures to reduce risks of possible compromise, or disclosure, to the manageable/acceptable levels. The level of protection is predicated on and commensurate with the value of the information and assets, or the probable harm that compromise, or disclosure would cause to national security. DoD and DON policy has been published defining Information Assurance (IA) strategy and features that are required. The strategy is a defense in depth scheme and the key features/requirements are confidentiality, integrity, availability, accountability, and non-repudiation.

In order that all Information Systems meet these criteria, a formal standardized process was developed to document and validate that all appropriate features and procedures were integrated into Information Systems and implemented and managed adequately. This process is required of all Information Systems and is embodied in the DoD Instruction 5200.40, DITSCAP.

The DITSCAP establishes standard processes, activities, and task descriptions to accredit Information Systems that will maintain the security posture of the Defense Information Infrastructure (DII). It is a tailorable process designed to certify that an IT system meets security requirements and that the system will continue to maintain the accredited security posture throughout the system life cycle. It consists of the following four phases and is a Site Representative, CDA, and/or PM responsibility:

1. Definition
2. Verification
3. Validation
4. Post-Accreditation

NMCI EDS will obtain accreditation for the NMCI network, and Navy NMCI DAA will therefore require that all Legacy Systems connecting to NMCI be accredited in order to connect and operate. Figure 3-1 illustrates this dependency. Note that the DITSCAP requires security testing (not to be confused with the NMCI "Certification" testing, which is a functional test procedure to ensure interoperability) as an integral part of the overall DITSCAP. DITSCAP security testing for Legacy Systems being integrated with NMCI is a Site Representative, CDA, and/or PM responsibility which must, along with the rest of the C&A process, be completed before the system can be accredited and connected to NMCI.

In the course of implementing NMCI, many valuable lessons have been learned about issues and activities related to transitioning to NMCI. Existing Navy systems/applications typically have not completed all DITSCAP and Navy IA Publications 5239-13 Vol. I & II requirements. Many systems/applications were developed or acquired prior to the existence or implementation of the DITSCAP and current Navy IA requirements. Other systems/applications have been provided to the Navy without all required supporting documentation. A result of this lack of detailed development information, systems engineering, and security documentation is that a secure means of transitioning to NMCI becomes difficult to define.

Rather than reverse engineer completely DITSCAP compliant documentation from existing documents and systems' owners and operators, NMCI PMO in coordination with CNO, Navy NMCI DAA, NMCI Cert Authority (SPAWAR PMW 161), and the USMC have developed a tailored approach to achieving an initial C&A document as a result of a process and activities described in the NSCAP.

The NSCAP defines those minimum NMCI IA requirements necessary for Navy IA compliance and to obtain DAA accreditation and to prepare that system's/application's owners, users, or developers for connection or transition to NMCI.

The NSCAP also provides the requirements for Legacy Systems/applications security C&A efforts in the Risk Mitigation phase of NMCI transition. It refines DON and USMC efforts to tailor DoD C&A requirements and activities while remaining DITSCAP compliant for existing fielded systems/applications. It also emphasizes reusing information from engineering activities, desktop application RCP activities, and any existing security or C&A documentation to augment compliance with DON and DoD requirements.

The end results of the NSCAP will be a required submission package (NSCAP Package) by the Site C&A Team to the office of the Navy NMCI DAA for review and adjudication on a transition request or a connection request.

C&A orientation will be part of Site Awareness and many aspects of the DITSCAP for each system can and should proceed in parallel with the data gathering and site survey activities, as has been indicated earlier. Legacy System Transition Team will be knowledgeable in this area and the PMO Enterprise C&A Coordinator has provided additional assistance and guidance to site personnel in accomplishing this requirement through the NSCAP Guide.

Further C&A activities have been incorporated in respective sections of the LSTG.

4.0 CONCLUSIONS

The LSTG serves as a roadmap in transitioning legacy systems to the NMCI environment, achieving the DON's end-state goal of one intranet for CONUS shore installations. With one centralized intranet, the DON will have visibility into the systems' total life cycle costs: equipment, licenses, maintenance agreements, and facilities. The end-state NMCI architecture is depicted in Figure 4-1.

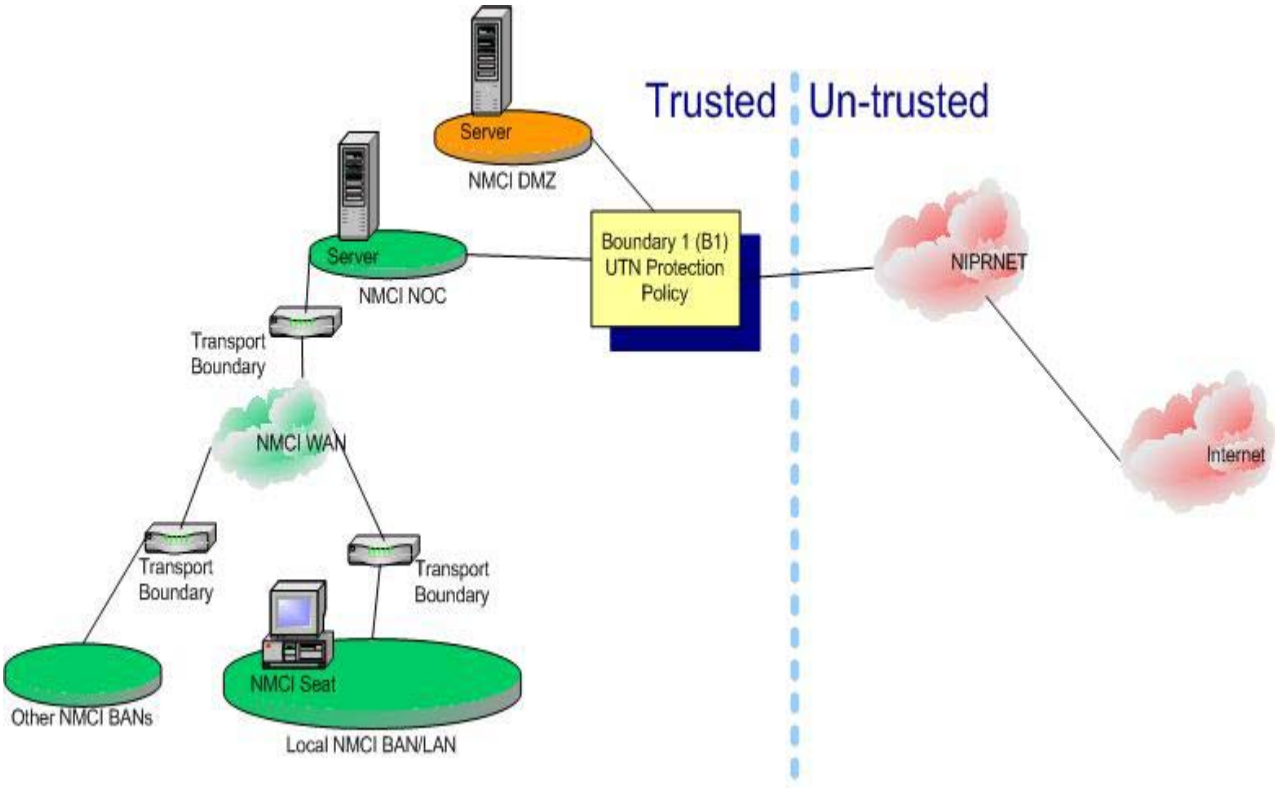


Figure 4-1 NMCI Architecture and Security Boundaries after Transitioning Systems

Having successfully transitioned "production or production ready" legacy systems to NMCI, the systems should demonstrate improved performance and availability, allowing the warfighter to focus on the mission rather than technology issues. The transitioned system residing in the NMCI environment realizes the following benefits:

1. Enhanced network security.
2. Interoperability across Commands and other Services.
3. Increased access to data across the globe.
4. Increased productivity.
5. Improved systems reliability and quality of service.
6. Centralized Administration and support for the Enterprise Network.

The Planning and Coordination Team will conduct an After-Action Review with the Site/System Representative, Legacy System Transition Team, EDS, and C&A Personnel to identify and document

lessons learned and process improvements associated with the Legacy System Transition Process. Future versions of the LSTG will incorporate lessons learned from System Transition pilot projects.

APPENDIX A: LIST OF RESOURCES

Point of Contacts:

- SPAWAR Program Management Office (PMO) – 858-537-0399, 619-524-7435
- Marine Corps Program Management Office (PMO)– 703-784-3788 (DSN 278)
- Electronic Data Systems (EDS) – 619-817-3487
- Applications Enterprise Action Group (AEAG) – 703-607-5653, 703-607-5654

APPENDIX B: ACRONYM LIST AND TERMINOLOGY

AEAG	Applications Enterprise Action Group
ATO	Authority to Operate
A-V	Anti-Virus
B1	Boundary One
B2	Boundary Two
BAN	Base Area Network
BLII	Base Level Information Infrastructure
BOM	Bill of Materials
CA	(1) Certification Authority; (2) Connection Approval
CDA	Central Design Authority
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CLIN	Contract Line Item Number
CM	Change Management
CNNOC	Commander, Naval Network Operations Command
CNNWC	Commander, Naval Network Warfare Command
CNO	Chief of Naval Operations
CO	Commanding Officer
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
CONOPS	Concept of Operations
CSU/DSU	Channel Service Unit/Digital Service Unit
C&A	Certification and Accreditation
DAA	Designated Approval Authority
DDAA	Developmental Designated Approval Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DNS	Domain Name Server
DoD	Department of Defense
DON	Department of the Navy
DON MC	Department of the Navy Major Claimant
DSL	Definitive Software Library
DMZ	Demilitarized Zone
ECCB	Enterprise Change Control Board
EDS	Electronic Data Systems Corporation
EMS	Enterprise Management System
ERQ	Engineering Review Questionnaire
FAM	Functional Area Manager
FTP	File Transfer Protocol

GOTS	Government Off-the-Shelf
GPO	Group Policy Object
HVAC	Heating, Ventilating and Air-Conditioning
IA	Information Assurance
IATO	Interim Authority to Operate
IATT	Information Assurance Tiger Team
IAVA	Information Assurance Vulnerability Alert (Message Alert issued by DISA WRT computer viruses)
IAVB	Information Assurance Vulnerability Bulletin (Message Bulletin issued by DISA WRT computer viruses)
IAW	In Accordance With
ILSP	Integrated Logistics Support Plan
INFOSEC	Information Security
IP	Internet Protocol
ISSM/O	Information System Security Manager/Officer
IT	Information Technology
IT-21	Information Technology for the Twenty-first Century
LAN	Local Area Network
LATG	Legacy Applications Transition Guide
LSTG	Legacy Systems Transition Guide
MTBF	Mean Time between Failure
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAVSO	Navy Staff Office
NCARP	NMCI Connection Approval Review Panel
NDAAL	Navy DAA Liaison
NEADG	Navy Enterprise Applications Development Guide
NEPP	Navy/Marine Corps Enclave Protection Policy
NISPOM	National Industrial Security Program Operating Manual
NMCI	Navy Marine Corps Intranet
NNOC	Naval Network Operations Command
NOC	Network Operations Center
NOIS	Navy Ordering Information System
NRDDG	NMCI Release Development and Deployment Guide
NRMP	Navy Release Management Process
NSCAP	NMCI Security Certification and Accreditation Process
O&M	Operations and Maintenance
OCONUS	Outside Continental United States
OS	Operating System
OPNAV	Office of the Chief of Naval Operations

OPNAVINST	Office of the Chief of Naval Operations Instruction
PDM	Product Delivery Manager
PDA	Product Delivery Analyst
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Point of Presence
PM	Program Manager
QA	Quality Assurance
QDATS	Quarantine Desktop Application Transition Strategy
R&D	Research and Development
RCP	Rapid Certification Phase
RFS	Remote Filing System
RMP	Release Management Process
R/W/B seat	Red/White/Blue seat
S&T	Science and Technology
SLA	Service Level Agreement
SM	Site Manager
SEM	Systems Engineering Management
SOP	Standard Operating Procedures
SOVT	System Operational Verification Test
SPAWAR	Space and Naval Warfare Systems Command
SSAA	System Security Authorization Agreement
ST-ERQ	System Transition Engineering Review Questionnaire
TART	Technical Applications Review Team
TB	Trust Boundary or Transport Boundary
TCP/IP	Transmission Control Protocol/Internet Protocol
TSS	Technical Support Staff
TTY	Text Telephony
TFWeb	Task Force Web
USMC	United States Marine Corps
ULSP	User Logistics Support Plan
UTAM	User to Application Mapping
VRU	Voice Response Unit
WAR	Weekly Activity Report

The following is a list of terms that are used throughout this document and accompanying appendices.

Application

- **Simple Application:** Unofficially, an application (COTS or GOTS) which runs on a desktop and does not have interdependencies with other applications and does not require network connectivity excluding printing. (Example, MS Word, Power Point, Excel, Flat Files).
- **Complex Application:** Unofficially, an application (COTS or GOTS) which runs on the desktop or server and has some interdependencies on other applications requiring network connectivity. (Example: Client to Server applications, database systems, thin client, thick client, and systems communicating over LANs, BANs, and WANs)

Application Interdependencies: as defined is an interface that an application has with any other application. This includes client to server and server-to-server dependencies.

Application Owner: as defined in the context of this document could be any one of the following:

- The Program Office of Record (POR) for development of a system/application, describing automated information system acquisition programs (ex. GCCS-M, ADNS, DMS, etc.) having a Navy budget line. Use in this document is consistent with Navy IA Pubs.
- The Central Design Activity/Agent (CDA) organization designated to design and develop software and supporting sub-systems.
- The Program Management Office (PMO) providing life cycle management to the system/application.

"As-Is" Legacy Network: Existing DON non-NMCI networks including backbone components. Typically, this is where Legacy Applications and Systems reside.

Boundary 1 (B1): Suite of network security components configured to provide perimeter security at the six NMCI NOC(s) connecting NMCI to the NIPRNET and SIPRNET.

Boundary 1 Firewall Policy: The security configurations and settings applied to the components of the B1 Firewall suite. It includes the Navy-Marine Corp. NIPRNET Firewall Configuration Baseline as part of the Navy-Marine Corp. NIPRNET Enclave Protection Policy, available for review in part at http://infosec.navy.mil or in full at https://infosec.navy.smil/mil.

Boundary 2 (B2): Suite of network security components configured to provide perimeter security at local sites connecting NMCI to legacy networks.

Boundary 2 Firewall Policy: Firewall policy implemented on B2. Specific to validated operational requirements between local "Trusted Enclaves" on NMCI and the local "As-Is" Legacy Network.

Boundary 3 (B3): Community of Interest (COI) separation from non-COI members within NMCI.

Boundary 4 (B4): Security Architecture providing server and desktop security.

Transport Boundary (TB): Suite of network security components configured to provide wide area network transport security.

Classification: Classification refers to the military status of this application. Is the application classified on un-classified.

Client Software: Refers to the software used on the client to access the application. For example: browsers, terminal emulation, or thick client.

Connection Type: Refers to the method in which the application or users are connecting to the network. Examples would include dial-up, TCP-IP, or DNS name servers.

Encryption: is used to protect unclassified within a computer system. This document asks specific questions related to the encryption compliance of the application. More information regarding the encryption requirements can be found at: http://csrc.nist.gov/cryptval/140-2.htm

EDS Site Solutions Engineering (SSE) Team: (with the assistance of the Application Owners) are responsible for:

- Collecting application information that will allow the PMO/IA Tiger Team to properly evaluate the application. Information is collected during the SSE Tier 2 process and is then compiled into a SWG package for review.
- Providing this information to the SWG Facilitator for distribution to the IA Tiger Team.
- Making sure that the Application Owners are aware of when their application is scheduled for review.
- Distributing Transition documents to Application Owners for verification.
- Obtaining signoff of the Transition documents.

Legacy Application (LegApp): Basically, any application (COTS or GOTS) not already provided under the NMCI standard desktop suite of applications or server services. A LegApp can be simple or complex.

Legacy Application Security Working Group (SWG): A working group made up of Information Assurance (IA) professionals from the DON and EDS that review legacy applications. These reviews are conducted every week with the Legacy Application Program Manager, Central Design Authority (CDA), users (Site personnel), EDS Site Solution Engineering teams, and other concerned personnel.

Legacy System: Unofficially, a collection of LegApps assembled to execute a function or task; includes hardware.

Mobile Code Requirements: Mobile code is software that enhances cross-platform capabilities, sharing of resources, and web-based solutions. Examples of mobile code include Java Code, Java Script or ActiveX. The **DoD Mobile Code Policy** defines the categories of mobile code and provides criteria for use within DoD. The policy can be found at the following link:
http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html

Network Architecture: A detailed network topology diagram that demonstrates the network connectivity of the system.

Network Placement: Detailed diagram that demonstrates where the servers/clients reside in relation to other network devices. If a determination can be made on the function of the components, this should be included. It is important to understand which system components are local and which are remote. This will also include data on component IP addresses and host names.

NMCI Certified: An abbreviated definition: A label given to Legacy Applications that EDS has tested and found to be compatible with Windows 2000, and NMCI Desktop Security, and which can be centrally

distributed using NMCI Centralized Management Tools. This is not the same as DoD Certification and Accreditation (DITSCAP).

NMCI Connection Approval Process (NCAP): Guidance provided to DON for gaining accreditation of legacy applications and interim approval to connect to NMCI.

NMCI Connection Approval Review Panel (NCARP): Panel of IT/IA professionals who assemble to review legacy application packages on behalf of Navy NMCI DAA for connection approval recommendations to Commander Naval Network Operations Command (CNNOC). Members include Naval Network Operations Command (NNOC), CNO N643, PMW-161, USMC, IATT, Site Representatives, and EDS in an advisory role.

NMCI Tier 1, Tier 2, and Tier 3 LegApp Reviews: Basically, the completion of LegApp questionnaires, and meetings designed to fully understand the design, communication requirements, and security impacts of Legacy Applications on NMCI.

Ports: Ports are used in network communications that cross boundaries/firewalls. Ports are also the point at which a communications circuit terminates/interfaces at a network device.

Protocol: A set of conventions that govern the instruction process, devices, and other components within a system [IEEE 90].

Services: These are network communication services that are used by the application/system. Examples include FTP, Telnet, and SMTP. In a layered network architecture, services refers to the boundary between functions of different layers. Commercially, the functions provided by a vendor of telecommunication services. For each service identified the following information is required:

Software version: The version of the application including information on patches that have been applied. (e.g. Oracle 8i, UNIX Version, System Utilities, etc.)

System: DoD Instruction Number 5200.40 describes a system as “A set of interrelated components consisting of mission, environment, and architecture as a whole.”

R/W/B seats: Definitions for R/W/B seats can be located at the corresponding CLINs. Red: Please refer to CLIN 0001AA / White: Please refer to CLIN1AB / Blue: Please refer to CLIN1AC.

APPENDIX C: SSAA

The DISA SSAA template tool may be found at: http://iase.disa.mil/ditscap/ditsssaa.html.

APPENDIX D: CLIN 29 REQUEST PACKAGE

The most current version of the questionnaire can be located at http://www.nmci-eds.com/CLIN29_Questionnaire.doc.

The information provided in CLIN 29 Request Package will be utilized by the Electronic Data Services to determine the appropriate price for your Legacy System. For information regarding the CLIN 0029 ordering process, please visit http://www.eds.com/nmci/clin029.htm.

APPENDIX E: EDS CLIN PACKAGE SCENARIOS

This appendix will be added to the LSTG when available.

APPENDIX F: LEGACY SYSTEM TRANSITION TEAM

1. EDS Teams

Many of the phase activities identified within this document require support by both EDS and the Government. This section is intended to identify some of the specific EDS teams as they apply to System Transition.

a. EDS Base Operations: Base Operations is responsible for customer-focused delivery of services. In this capacity, the team ensures regular customer communication and provides information regarding site and customer status to EDS. Site Managers deployed by Base Operations are the primary Points of Contact (POCs) at an installation for NMCI. They manage "As-Is" concerns for a site, are supported by the Legacy System Transition Team in the move to the end-state environment, and manage the end-state environment on an ongoing basis. EDS Base Operations is the primary channel for customer requirements.

b. The Business Office is the centralized entity that is responsible for proposal creation in response to a CLIN request. In this capacity, the team ensures requirements have been defined and provides a proposal based on those requirements. The Business Office will engage appropriate EDS and government resources when necessary to complete the proposal.

c. NMCI Help Desk: The NMCI Help Desk is designed to provide the initial support whenever a user encounters an issue with the operation of their desktop.

- Conduct an initial assessment of the problem
- Provide basic support for desktop operations
- Initiate Remedy tickets for more complicated issues

d. Network Operations Center (NOC): The NOC performs Enterprise Management and is responsible for monitoring the network, network operating systems, servers, event correlation, and inventory collection. The NOC's objective is to provide operational support to the client as well as to NMCI staff.

2. Site/ System Representative

a. Site Representatives: The Site Representatives have the responsibility to represent the User Community by:

- Determining information system security requirements [IA Pub-5239-13 Vol. II]
- Facilitating support for all infrastructure/facilities support
- Providing hardware to support system technical architecture, when applicable
- Serving in a leadership role and decision authority on every Legacy System Transition Team, except the Site Visit Team
- Completing the ERQ or ST-ERQ (System Transition Engineering Review Questionnaire)
- Providing system security documentation for servers (SSAAs, network drawings, system architectural documents, etc.)

b. CDA: For the purposes of this guide, a CDA is anyone (any organization, site, group, department, division, unit, section, individual, government, government sponsored contractor) who desires to introduce a new application or change an existing application within NMCI environment. CDAs are responsible for ensuring that releases are compliant with Navy information assurance, boundary, and Group Policy Objective (GPO) policies prior to deployment within NMCI. CDAs must keep in mind the requirements for developing and migrating applications to comply with Task Force Web (TFWeb), NMCI, Information Technology for the 21st Century (IT-21), Outside-Continental United States (OCONUS) Base Level Information Infrastructure (BLII) architectures, and DON standards NRDDG.

c. PM: The PM is the person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the Information Technology (IT) system. [DoD Instruction Number 5200.40 and IA Pub-5239-13 Vol. I] Typically, the Navy refers to this role as the POR and the Marine Corps refers this role as the PM.

d. Also, the PM is the Certification Authority and system/component developer responsible for ensuring the security design. The DAA, CA, and Certification Agent interact with the PM to support requirements definition and security engineering. [IA Pub-5239-13 Vol. I]

e. The respective system Site Representative, CDA, and PM serve in a leadership role and decision authority on every Legacy System Transition Team, except the Site Visit Team.

f. Site C&A Team: The Site C&A Team functions at the Site level and is composed of the Site Designated Approval Authority (DAA), Site Information Security System Manager (ISSM), Site Information System Security Officer (ISSO), etc.

3. C&A Personnel

a. Certification Agent: The Certification Agent is the individual(s) responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages to include the SSAA. This role may be assigned to various entities based upon complexity of the certification level of effort. [IA Pub-5239-13 Vol. I and NAVSO P-5239-02]

b. The Certification Agent supports the Certification Authority in verifying the security requirements. The Certification Agent supports the PM by providing security engineering during the development of the system/component and assists in development of the SSAA for submission to the DAA. For the purposes of the LSTG and the NMCI transition the Certification Agent will provide guidance and expertise to the PM in the preparation and submission of the NSCAP package.

c. Developmental DAA: The DDAA supports the program acquisition during the design and development of a system/component and accredits systems prior to their deployment. The Operational DAA is the ultimate approving authority for system operation at a specific site. [IA Pub-5239-13 Vol. I] For the purposes of the LSTG, the Operational DAA is the Navy NMCI DAA.

d. Certification Authority: The Certification Authority is the official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meet a set of specified security requirements. [DoD Instruction Number 5200.40]

e. Also, the CA reviews the C&A package prepared by the Certification Agent and issues the certification statement. [IA Pub-5239-13 Vol. I]

- Review and endorse the NSCAP/NMCI Connection Approval Review Panel (NCARP) Package
- Review and approve C&A POA&M
- Review and endorse transition/connection recommendation
- Review Legacy System Transition POA&M
- Coordinate and archive transition/connection requirements if restrictions are levied

f. Navy NMCI DAA: The Navy NMCI DAA (Operational DAA) is the official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. [DoD Instruction Number 5200.40]

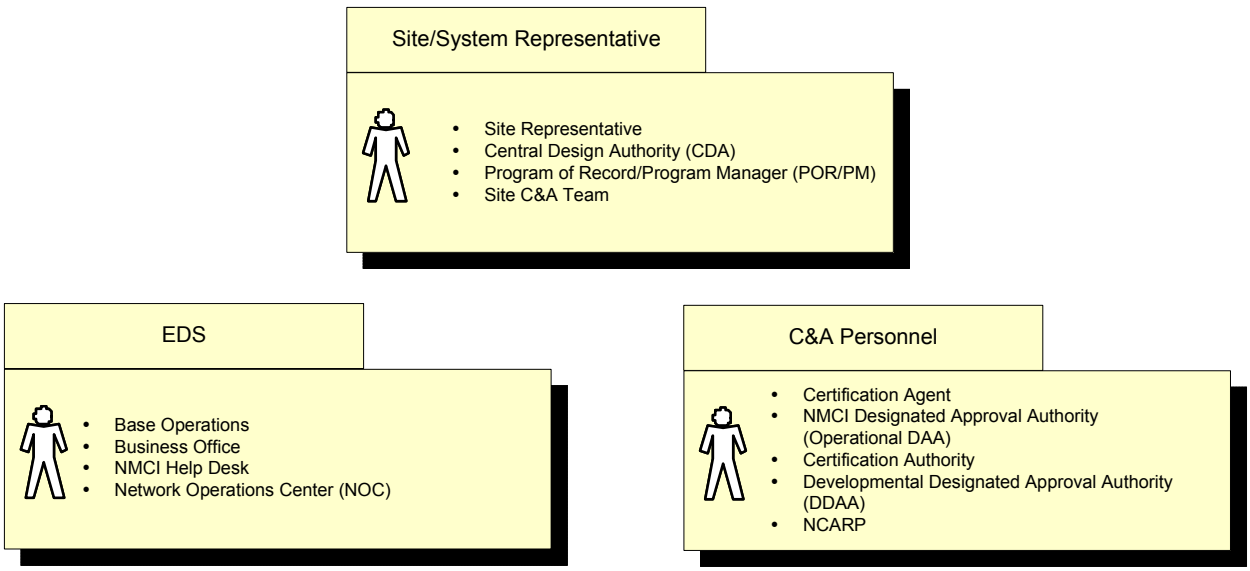
The DAA is responsible for ensuring compliance with the DON INFOSEC Program for the activities and information systems under the DAA's jurisdiction. The DAA grants interim and final approval to operate an information system in a specific security mode based on a review of the accreditation documentation and a confirmation that the residual risk is within acceptable limits. [NAVSO P-5239-07]

The Navy NMCI DAA is responsible for the overall security posture of the NMCI enterprise and will be the Navy's final decision authority to either disallow or grant:

- Conditional Approval to Transition to NMCI
- Unconditional Approval Transition to NMCI

g. NMCI Connection Approval Review Panel (NCARP)

Legacy Systems Transition Supporting Personnel



APPENDIX G: POA&M

LSTG: Transition POA&M

"Updated POAM.mpp"

This template provides a standard POA&M that encompasses all phases of migrating a system into NMCI. For each system(s) to be migrated, the POA&M needs to be tailored to meet the scope of the effort as defined by the customer's requirements. Once the customer's requirements have been defined, documented and approved by the customer, the POA&M is tailored to fit the effort. Tailoring will consist of the following activities:

- Determining the applicable activities and/or deliverables
- Eliminating the activities and/or deliverables that do not apply
- Adding activities and/or deliverables that are specific to the site or system that are not standard across all projects
- Assigning resources to site or system specific activities

APPENDIX H: RISK MANAGEMENT ASSESSMENT TOOLS

The following tools have been selected for NMCI activities in site evaluation and risk mitigation. Results gathered from these tools are utilized in facilitation of the NSCAP materials for the planned transition.

Internet Scanner: Internet Scanner is a product of Internet Security Systems (ISS). Internet Scanner provides network vulnerability assessment for measuring security risk. This type of software is generally referred to as a scanner. The results of the scan are saved to the hard drive of the host laptop and then reports can be generated. The reports also provide risk remediation advice.

DISA Security Readiness Review (SRR): DISA SRR are scripts created by DISA that are run on the servers. The results of the scan provide the information on DISA STIG and IAVA compliance. The results of the scan are saved on the server then moved to a workstation so reports can be generated.

APPENDIX I: PROJECT MILESTONES AND DOCUMENT DELIVERY CHECKLIST

The LSTG: Project Milestones and Document Delivery Checklist

"LSTG Project Milestones and Docu

APPENDIX J: COST ESTIMATE MODEL

"Cost Estimating for Leg Sys Tr_v6FINAL1

"NMCI_Cost_Estimate_Tool_v1-6 14OCT0

APPENDIX K: ST-ERQ (AUGMENTED TO INCLUDE ENTIRE SYSTEM)

The System Transition Engineering Review Questionnaire (ST-ERQ) is attached.

"System Transition Engineering Review (